SWITCH security report on the latest IT security and privacy trends

November/December 2019

SWITCH

I. Is internal security just an issue for security companies?

Security companies are considered close allies of users in the fight against hackers, spammers and other cyber criminals. Around the world, more than 12 million customers rely on cybersecurity products from the Japanese company Trend Micro, for instance. In August 2019, Trend Micro itself fell victim to a cyber attack. But not just any cyber attack – one from within. In early November, threatpost reported that a rogue employee had gained unauthorised access to a database and had stolen and sold on the names, email addresses, support ticket numbers and – in various cases – phone numbers of 68,000 customers contained in the database. Soon after, the victims of this data leak were called by fraudsters posing as Trend Micro’s support staff. Some of the customers who had been called contacted the company, which opened an investigation and confirmed that the data had been stolen in early November, but it was unable to disclose who had bought it.

Like data from online and social media platforms, customer data from security companies is extremely valuable and a gold mine for internal criminals. In the same post, threatpost announced that Snap and Facebook also had problems with employees abusing their access to customer data. The Verizon Data Breach Investigations Report 2019 estimates that insider threats account for almost one third of all data leaks.

In view of this threat situation, it is even harder to understand why some companies are so frivolous (not to mention sloppy) when it comes to dealing with their customers' data. Take for example the French Gekko Group's hotel booking platform, which specialises in arranging business trips. It stored more than a terabyte of booking information, credit card details and access credentials for AccorHotels customers and various subcontractors, especially Teldar Travels and Infinite Hotels, in an unprotected and unencrypted Elasticsearch database. While Gekko claims that it secured the server, it certainly isn't the only company that is sloppy and reckless with customer data. In October, nearly 7.5 million Adobe Creative Cloud customer accounts were also visible online, unprotected, in an open Elasticsearch database.

And Wizards of the Coast – developer of the popular 'Magic – The Gathering' trading card game – also stored a database backup in the cloud, where it was unprotected and freely accessible. The backup contained more than 452,000 user accounts for the online game, including email addresses and hashed passwords. Wizards of the Coast claimed that it was aiming to inform the players affected and prompt them to change their passwords. And because Brexit hasn't been implemented yet, there is also evidence in this situation of a major reportable and sanctionable incident under the European General Data Protection Regulation.

Conrad Electronic, the electronics mail order company, learned in November that targeted external attacks can be immensely successful despite all its precautionary measures. It emerged that unknown attackers had exploited a security gap in the Elasticsearch database, allowing them to spend months extracting nearly 14 million customer data records from the multi-channel retailer's systems. Although they didn't take credit card information or customer passwords, the hackers did manage to steal postal and email addresses, fax and phone details and – in about 280,000 cases – IBAN numbers.

The security gap was closed in this case too. The company owner apologised to its customers and informed them that it had filed a criminal complaint and notified the data protection authorities as required by the GDPR.

Read more:

https://threatpost.com/trend-micro-rogue-employee-68k-customers/149946
https://threatpost.com/verizon-dbir-espionage-c-suite-cloud/144486
https://www.heise.de/newsticker/meldung/Datenleck-Kundendaten-von-Hotelbuchungsplattform-ungeschuetzt-im-Internet-4592945.html
https://techcrunch.com/2019/11/16/magic-the-gathering-wizards-data-exposure
https://www.heise.de/newsticker/meldung/Unbekannte-dringen-in-Server-von-Conrad-Electronic-ein-4591326.html

II. CNAME cloaking – the new privacy attack

Ever since he was associated with the Cambridge Analytica scandal surrounding the last US presidential election, if not before, many critics have considered Michał Kosiński to be a gravedigger of privacy. In an interview with the Swiss daily newspaper *NZZ*, he said that we should wave goodbye to our privacy, so that the positive outcomes of digitalisation can be put to better use. But he also added it would help in dealing more impartially with the threat posed by AI, which he believes to be far more serious.

The professor of psychometry, now a lecturer at Stanford University, may have been playing into the hands of the traditional tracking companies (quotation: Mike Kuketz, kuketz-blog.de, link below), who have found a new way of tracking us and sneaking ads past ad blockers in the form of CNAME cloaking. Why? Because despite all the ad blockers and add-ons for web and mobile browsers, online advertisers are still chasing user data and attention like the orcs tailing the Fellowship in the Mines of Moria. And that's why they're always on the hunt for new ways to trick sophisticated ad blockers and add-ons. Now it seems that advertising companies like Eulerian (which, besides Warner Brothers, also has major French brands from Canal+ to the F. Leclerc supermarkets among its testimonials) have found a way to tricks almost all common anti-tracking efforts with CNAME cloaking.

CNAME stands for 'canonical name and cloaking for camouflage', and it isn't clear whether Eulerian is simply arrogant and cynical in listing 'transparency' as one of its four company values on its own website, or if it has completely lost touch with reality. Because the name says it all – common ad blockers or built-in tracking protection routines protect against known advertising and tracking domains. But only them. However, if they pop up time and again under new names randomly generated in the Domain Name System (DNS), the anti-tracker has no chance of recognising them as the advertising website it is designed to block. Currently, only the uBlock origin add-on for Firefox version 60 or higher, which is currently only available in beta version, is capable of preventing tracking using CNAME cloaking. This is the assessment of Mike Kuketz, a security blogger, penetration tester and employee of the Baden-Württemberg State Commissioner for Data Protection and Freedom of Information. uBlock origin uses a programming interface that can resolve the host names of a DNS entry and thus expose the actual sender. Google's Chrome and Apple's Safari do not have a comparable interface, so they cannot expose CNAME trackers. Chrome doesn't even appear to want to any more, with the Google 'Manifest v3' stating that Chrome add-ons will only be able to read browser requests in future, not change or even block them.

Read more:

https://www.nzz.ch/feuilleton/michal-kosinski-facebook-ist-phantastisch-fuer-die-demokratie-ld.1520699
https://www.heise.de/newsticker/meldung/Firefox-uBlock-Origin-schuetzt-vor-versteckten-Trackern-4596641.html
https://tarnkappe.info/cname-cloaking-neue-tracking-methode-trickst-adblocker-aus
https://medium.com/nextdns/cname-cloaking-the-dangerous-disguise-of-third-party-trackers-195205dc522a
https://www.theregister.co.uk/2019/11/21/ublock_origin_firefox_unblockable_tracker

III. Emotet (& others): a devastating malware cocktail – now with added NextCry for Linux

In the last SWITCH security report, for the second time this year we highlighted the immense damage caused across the board by the Emotet Group's ransomware. We are issuing this – our third warning about ransomware in a short space of time – because the chain of attacks described in the last report (and again in detail at the first heise.de link below) is still active and still highly dangerous. In a nutshell, the initial compromise involves personalised spam emails being sent from exposed representatives of companies or organisations, asking employees to open an infected Word attachment that Emotet uses to access the employees' Windows computers. TrickBot is then downloaded to retrieve account credentials, move laterally on the victim's systems and discover, for example, how the backup systems work. In the third step, the encryption trojan Ryuk is downloaded. Thanks to its integrated worm component, it can eat its way through the entire network and encrypt all of the data it contains. CERTs and IT security organisations sometimes describe this cocktail as one of the most destructive and costly attacks ever.

Its most recent victim was Prosegur, the global Spanish security service, whose 175,000 employees in 25 countries provide personal protection, security services, money and valuables transportation, plus alarm systems planning, installation and maintenance. In late November, Prosegur reported an Emotet/TrickBot/Ryuk attack, which brought the company to a standstill in some areas. A good 24 hours later, the company announced that it had identified and averted Ryuk, but not all services were fully available.

While Emotet and other attackers are ravaging the Windows world, Linux users also have real cause for concern, because they're the target for Nextcry, which has been using blackmail to wreak havoc since mid-November. This development was reported by security website bleepingcomputer.com in mid-November. Apparently, the attackers had used a vulnerability (now patched) in the FastCGI process manager PHP-FPM (CVE-2019-11043) of Nextcloud servers with NGINX as a reverse proxy to encrypt the stored data in such a way that it can no longer be decrypted without a ransom payment. In its own blog, Nextcloud discusses security updates and points out that two out of 300,000 Nextcloud servers have been hacked without a ransom being paid. At the same time, the provider confirms that the importance of IT security cannot be overestimated. Given the damage that ransomware causes, we've got nothing more to add to that.

Read more:

https://www.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html
https://www.zdnet.com/article/security-firm-prosegur-weve-shut-our-it-network-after-ryuk-ransomware-attack
https://www.heise.de/newsticker/meldung/Sicherheitsvorfall-beim-Sicherheitsdienst-Ransomware-Ryuk-befaellt-Prosegur-4598361.html
https://www.bleepingcomputer.com/news/security/new-nextcry-ransomware-encrypts-data-on-nextcloud-linux-servers
https://www.heise.de/security/meldung/Ransomware-NextCry-greift-Nextcloud-Server-an-4588421.html
https://nextcloud.com/blog/nextcry-or-how-a-hacker-tried-to-exploit-a-nginx-issue-with-2-nextcloud-servers-out-of-300-000-hit-and-no-payout

IV. Account deletions and the tough battle against fake news on social media platforms

In a new development, Twitter and Instagram want to delete inactive accounts, but are on the receiving end of some angry protests from account holders. While users generally didn't respond to Twitter's announcement that it would delete inactive accounts to 'distribute more accurate, credible information that people can trust on Twitter', the Adult Performers Actors Guild (APAG) protested that Instagram had deleted more than 1,000 of its members' accounts because they felt they had violated community rules. The protesters accused the social media platform of double standards because, in many cases, it had no problem at all with publishing misogynistic content. Instagram's rules generally stipulate that it will not host nudity in the form of photos, videos or other digital content. However, these rules obviously don't apply to all users to the same extent.

Inconsistencies and contradictions concerning the application of guidelines in the (non-) publication of content is also leading to discussions on other social media platforms. In an article on newscientist.com, Donna Lu, for instance, doubts that Facebook's efforts to contain fake news by deleting fake accounts, among other things, could be considered a success. She points out that the social media giant – quietly and secretly – had substantially watered down its advertising guidelines in October, which had been tightened up in the wake of the Cambridge Analytica scandal and the calls for the break-up of Facebook. She also queries how the two monitoring partners that Facebook wanted to use in the run-up to the British parliamentary elections intended to sift through the billion daily posts when the larger of the two partners employs fewer than ten people.

And companies that have sent newsletters to thousands of subscribers using WhatsApp are perplexed and – to put it mildly – angry at the messenger service, which is part of the Facebook empire, because from 7 December 2019 the company will definitively stop sending these newsletters and will punish them by taking legal action starting with account blockage, with reminders sent at a fee. What is interesting about all of this is that newsletter mailing has always violated WhatsApp's terms and conditions.

Read more:

https://futurezone.at/digital-life/twitter-loescht-profile-die-ein-halbes-jahr-inaktiv-sind/400687487
https://futurezone.at/digital-life/accounts-geloescht-pornostars-beschweren-sich-ueber-instagram/400687316
https://www.newscientist.com/article/2221963-facebook-has-a-plan-to-tackle-fake-news-heres-why-it-wont-work
https://www.internetworld.de/online-marketing/whatsapp/whatsapp-newsletter-firmen-7-dezember-tun-1727506.html

This SWITCH security report was written by Dieter Brecheis and Frank Herberg.

The SWITCH security report does not represent the views of SWITCH; it is a summary of various reports published in the media. SWITCH assumes no liability for the content or opinions presented in the security report nor for the correctness thereof.