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

May / June 2019

SWITCH

I. Brought to light: Federal Crime Office closes down the world's second largest illegal dark web marketplace

Even bad guys have business models – or at least imitate those of the good guys. Criminals on the dark web use e-commerce, encryption technologies, anonymised browsers and cryptocurrencies like bitcoin, ethereum or monero to run what are basically gigantic trading platforms. Deals worth many millions are made on these platforms, involving drugs, weapons, human trafficking, illegal pornography, malware and other illegal goods and services, such as stolen login credentials, cyberattacks and botnets. For example, the Silk Road marketplace, which was shut down in 2013, turned over more than USD 1.2 billion in just two years and reportedly generated around USD 80 million in commission fees for its American founder and proprietor, Ross Ulbricht. Such lucrative prospects certainly motivated many Germans to do the same. The operators of Hansa Market, which was discovered in 2017, are now in custody, for example. They also generated billions in turnover and made millions on commission fees.

No sooner were they behind bars than the next dark web market, known as 'Wall Street Market', emerged – once again, in Germany. This platform also quickly became a sales powerhouse with impressive business figures: 1.1 million registered users and approximately 1,250 daily transactions with 63,000 listings, totalling 400,000 sales transactions, 250,000 of which were for narcotics or, in other words, drugs. By comparison, the largest legal online marketplace in Switzerland, ricardo.ch, has 3.2 million members and receives about 360,000 visitors per day. While the figures for the legal portal were self-reported, the figures for Wall Street Market were released by Germany's Federal Criminal Police Office (Bundeskriminalamt – BKA).

At a press conference on 3 May 2019, the BKA announced that it had closed Wall Street Market after an 18-month investigation in cooperation with the German Central Office for Internet Crime (ZIT), Europol, and Dutch and American authorities. Three Germans aged between 22 and 31 were also arrested. They are suspected of running the illegal dark web platform and collecting between 2 and 6% in commission fees. If found guilty, they face up to 15 years in prison (by comparison, Silk Road founder Ross Ulbricht was given a life sentence). A search of their homes turned up more than half a million euros in cash, piles of documents relating to large amounts of the cryptocurrencies bitcoin and monero, and a firearm – all of which strengthens the case against them. It was initially unclear whether the investigators also managed to crack the seized servers and access their data on up to 5,400 sellers and more than a million users, in order to prosecute them. What is known, however, is that the investigation led to the arrest of two of the most active sellers in Los Angeles. When Wall Street Market was closed, Europol announced that it had also shut down the Finnish dark web marketplace Silkkitie, also known as Valhalla Marketplace. The next copycats are probably just biding their time.

Read more:

https://m.tagesanzeiger.ch/articles/28284916
https://help.ricardo.ch/hc/de/articles/115002981745-Überblick-ricardo-ch-AG
https://techcrunch.com/2019/05/03/how-german-and-us-authorities-took-down-the-owners-of-darknet-drug-emporium-wall-street-market
https://www.heise.de/newsticker/meldung/Wall-Street-Market-BKA-und-FBI-heben-illegalen-Darknet-Marktplatz-aus-4412205.html

II. WhatsApp, state trojans? Or, why the city of San Francisco protects privacy better than Mark Zuckerberg's messenger app

Two privacy-related news items that recently came out of California couldn't be further apart on the spectrum. First, the bad news: in mid-May, the WhatsApp messenger service, owned by Mark Zuckerberg's Facebook, reported a security hole that could be exploited to install spyware on iPhones, Android and Windows smartphones, as well as TV devices running Samsung's Tizen operating system. WhatsApp has since closed the security hole but recommends that all users install the relevant update.

Security experts believe that the hole was used not for a widespread attack but rather for targeted attacks on specific phones, particularly those of lawyers and employees working for human rights organisations. The highly sophisticated spyware could be sneaked onto hacked phones simply by making a voice call – even if the person called did not answer. The calls were also deleted from the phone's log files. It appears that the malware would have allowed the attacker to activate the camera and microphone of the infected smartphone and to access emails, messages and location data. According to the *Financial Times*, a London-based human rights lawyer was one of the targets, but fortunately his phone was highly secure, ultimately foiling the attack.

All of this led experts to the conclusion that the spyware had been developed by the Israel-based NSO Group. Valued at USD 1 billion, the software company markets its flagship product Pegasus in the Middle East and to western intelligence agencies as a piece of spyware to combat terrorism and other crime. The lawyer who was targeted in the attack had represented several Mexican journalists and a Saudi dissident in a lawsuit against NSO. Responding to enquiries, NSO said it offers its software to secret services and security agencies but does not use it itself.

The good news in the realm of privacy is also from California. On 14 May, the local Board of Supervisors passed legislation prohibiting police and other municipal authorities from using surveillance technologies of all kinds – from facial recognition software to licence plate scanners – anywhere in the city, or at least requiring them to have permits to do so. Currently, the law does not apply to private companies, seaports and airports where these technologies are being used. Other cities in the United States are also considering whether to expand privacy protections by restricting surveillance technologies. In Washington, Congress is also discussing a proposal to prohibit private companies from taking pictures of and using facial recognition on consumers without their consent. Facial scanning is not only part of the discussion because of its widespread use – for example, in China, it has led to a total surveillance state – but also because it is (still) relatively unreliable. For example, the NZZ on 4 May and the SRF programme '10 vor 10' on 3 June 2019 both reported that the Uighurs and Muslims who make up the majority of the population in Xinjiang province live under almost total surveillance owing to facial recognition and a smartphone app. Remember, too, the story in our 6/2018 security report of how one of the most famous entrepreneurs in China was publicly chastised by mistake after automatic facial scanning software had recognised her face in an advertisement on the side of a passing bus and issued a citation for unlawfully crossing the street on red.

Read more:

https://www.nzz.ch/digital/sicherheitsluecke-bei-whatsapp-ermoeglichte-die-installation-von-ueberwachungssoftware-ld.1481584
https://www.spiegel.de/netzwelt/apps/whatsapp-sicherheitsluecke-ermoeglichte-gezielte-ueberwachung-update-noetig-a-1267300.html
https://www.nzz.ch/international/san-francisco-verbietet-gesichts-scanner-ld.1481881
https://www.faz.net/aktuell/politik/gesichtserkennung-in-china-totale-kontrolle-15253415.html
https://www.nzz.ch/international/xinjiang-die-polizei-hat-die-uiguren-mit-einer-app-im-griff-ld.1479234
https://www.srf.ch/play/tv/sendung/10vor10?id=c38cc259-b5cd-4ac1-b901-e3fddd901a3d
https://securityblog.switch.ch/2018/12/20/the-november-december-2018-issue-of-our-switch-security-report-is-available

III. Privacy at Facebook, part two: when the lawyer contradicts the boss

During Facebook's F8 developer conference, Mark Zuckerberg surprised everyone – friends and critics alike – by announcing 'the future is private!' Was this merely a new marketing gimmick, or had the scandals swirling around the data vacuum's lax handling of users' private data over in Menlo Park forced the company's boss to rethink things? Those who were listening must have initially assumed the latter. Zuckerberg announced nothing less than his company's strategic shift away from the 'digital marketplace' and more towards a 'digital living room'. In the future, Facebook companies will supposedly pay more attention to privacy. For example, end-to-end encryption is to be used not only for WhatsApp but also for Messenger. It remains to be seen whether the company can win back its users' lost trust to launch new products, such as a direct shopping feature in Instagram or a separate dating platform.

With this in mind, the statement made by Facebook lawyer Orin Snyder during a court hearing in San Francisco is unlikely to help boost sales. During the hearing on the Cambridge Analytica scandal, he argued: 'There is no invasion of privacy at all, because there is no privacy.'

Read more:

https://www.faz.net/aktuell/wirtschaft/diginomics/entwicklerkonferenz-von-facebook-die-zukunft-ist-privat-16165374.html
https://www.heise.de/newsticker/meldung/Facebook-Rechtsanwalt-Es-gibt-keine-Privatsphaere-4436701.html

IV. Symmetry as a fundamental principle: now that we have software as a service, it is only a matter of time before we have cybercrime as a service

As the first section of this article illustrated, symmetry is a fundamental principle of order in our world: yin and yang, light and dark, good and evil are found in the digital world, too. A recent example was the announcement, in mid-May, by the US Department of Justice and Europol that, through a joint covert operation, they had arrested the network of cyber criminals behind the Goznym malware and the Avalanche botnet, discovered two years earlier. The malware had, up to that point, already infected more than 41,000 computers and attempted to steal an estimated USD 100 million from its victims. The full extent of the damage has not yet been determined.

However, it was discovered that the perpetrators built and operated a network involving some highly specialised cyber criminals. Steven Wilson, Head of the European Cybercrime Centre, described it as a 'supermarket for cybercrime services'. Each specialist was responsible for only a part of the operation. All of the parts were then linked together in a supply chain of sorts. The programmers, malware developers, bulletproof hosters and other criminals from Russia, Ukraine, Bulgaria, Moldova and Georgia offered "cybercrime as a service" in hard-to-access online forums. Symmetry is ubiquitous – including on the dark web.

Read more:

https://www.europol.europa.eu/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation
https://www.wired.com/story/goznym-takedown-cybercrime-supply-chain
https://www.heise.de/newsticker/meldung/Malware-Attacken-ueber-Avalanche-Botnet-Drahtzieher-vor-Gericht-4423942.html

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

The SWITCH-CERT 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.