SWITCH Security Report on current trends in the field of IT security and privacy

September/October 2023

I. You better look a gift horse in the mouth: Phishing with caravan and motorhome offers

The offer of the advertisement on second-hand vehicle portals sounds tempting: because they have supposedly emigrated and no longer have a need, a couple wants to give their older used leisure vehicle to a needy family or sell it at very favourable conditions. To prove the credibility - in both senses of the word - of the request, the advertiser claims that she and her husband are Bible-believing Christians who are serious and do not want to play with people's feelings. What sounds too good to be true is also true: At the beginning of October, the police warned that these are bait-and-switch offers with which gullible victims are usually doubly harmed:

On the one hand, they are asked to send their personal data together with a copy of their passport or ID card because the vehicle is abroad. The data obtained in this way is later used for other offences not specified by the police.

Secondly, in the course of the further purchase process, the scammers inform the victims that transport and customs fees would be incurred for the export of the vehicle. Once the victims have transferred the money, the scammers break off contact and the victims' data and money are lost. In the worst scenario, the passport photos are then also used to produce and distribute

deep fakes.

The current cases show that such so-called "impersonation attacks" are increasingly being observed. In an interesting blog post linked below, the security company UpGuard has clearly listed the different forms of such attacks and described how users can protect themselves from them.

Read more at:

https://www.cybercrimepolice.ch/de/fall/lockvogel-inserate-mit-wohnmobilen-und-wohnwagen
https://polizei.news/2023/10/11/betrugsmasche-lockvogel-inserate-mit-wohnmobilen-und-wohnwagen
https://www.upguard.com/blog/impersonation-attack#:~:text=An%20impersonation%20attack%20is%20a,giving%20up%20sensitive%20information%2C%20or

II. Holiday recap of the criminal kind: Sophisticated attacks on hotels, travel agencies and booking platforms

In a completely different and extremely sophisticated way, a multi-stage wave of attacks against hotels, travel agencies and booking platforms has been going on since September. Here, too, the goal is to capture sensitive data - in this case, the complete credit card data. As the security company Perception Point reports, the cybercriminals are particularly sophisticated and extremely cautious in their approach by first sending a booking request to a hospitality company (hotel or travel agency). In response, they send a very personalised and emotionally touching email with an additional question or a special request and a link to a file sharing service. To underline their credibility, they also send a clear-text password with which the attacked company can log on to the file server and download a compromised archive - and thus a spying and data theft software.

Once executed, the cybercriminals click into the victim's customer data and start a direct dialogue with these customers. After a supposed system update, they are asked to send further necessary data of their credit card so that the booking can remain valid. The link sent along leads to a deceptively real-looking, but fake booking.com page. As Perception Point writes, the campaign is already above average in its multi-stage design. In addition, the individual stages of the attack are also extremely sophisticated and skilfully executed.

The cyber extortionists of the Russian RaaS (Ransomware-as-a-Service) provider ALPHV, or their "system partner" known as Scattered Spyder, apparently managed to compromise the MGM casinos and hotels in Las Vegas much more easily. On 13 September, the e-gangsters posted on X that it had taken them just a ten-minute phone call to a casino's help desk to take control of the systems of the 33.9 billion US dollars entertainment company. While MGM had initially stressed that operations were largely unaffected, on 6 October the group published the damage total of 100 million US dollars and announced that customer data had also been stolen. ALPHV

is also known as BlackCat, ALPHV-ng or Noberus and has been operating in an elevated capacity since 2021. The group and its clients mainly attack large organisations and companies, relying on triple extortion: after infiltrating the systems, sensitive data is stolen. Then the criminals encrypt the victim's systems and demand a ransom for decryption. To lend weight to the demand, they threaten to publish the stolen sensitive data. And if the victim still does not pay, he is threatened with a DDoS attack. In addition, security researchers consider ALPHV to be extremely professional in the use of social engineering techniques, e.g. in obtaining secret access data through cleverly conducted telephone calls or emotionally touching e-mail exchanges. Because the group is also highly skilled in using exceptionally well-functioning malware tools, security researchers and law enforcement agencies conclude that it is made up of former members of the cybercriminal group REvil, which was dismantled by Russian authorities in 2022, as well as actively recruited BlackMatter and DarkSide members.

Latest victim in Europe: The Motel One Group was attacked by ALPHV at the end of September. The European hotel chain with headquarters in Munich operates the 90 hotels in 13 European countries. Among them are one each in Zurich and Basel. While Motel One claimed in an initial statement on 2 October that it had managed to keep the impact of the attack "relatively low", the blackmailers themselves had boasted that they had captured more than 6 terabytes of sensitive data in about 25 million files. These included the company's business figures, employees' mobile phone numbers, private and business billing addresses, customers' birthdays, accommodation lists and the data of about 150 credit cards. In the days after the hack, it turned out that the cybercriminals could for once claim to be on the honest side: The data has since been published on the Darknet. Motel One founder and co-owner Dieter Müller has meanwhile admitted that the affected customers had been informed and assured politicians that "... cyber defences will be upgraded considerably". Until this is done, anyone who has stayed at a Motel One since 2016 should be especially careful and sensitive if he or she is contacted by unknown persons: it could be a phishing attempt.

Read more at:

https://perception-point.io/blog/stealing-more-than-towels-the-new-infostealer-campaign-hitting-hotels-and-travel-agencies
https://www.bleepingcomputer.com/news/security/hotel-hackers-redirect-guests-to-fake-bookingcom-to-steal-cards
https://www.engadget.com/hackers-claim-it-only-took-a-10-minute-phone-call-to-shutdown-mgm-resorts-143147493.html
https://twitter.com/vxunderground/status/1701758864390050145?s=46&t=mOWjpAvBR_EgMxB3MbSPxw
https://www.varonis.com/de/blog/alphv-blackcat-ransomware
https://www.bleepingcomputer.com/news/security/mgm-resorts-ransomware-attack-led-to-100-million-loss-data-theft
https://www.inside-it.ch/wir-haben-6-terabyte-daten-ransomware-bande-droht-europas-grosser-hotelkette-motel-one-20231002
https://www.golem.de/news/motel-one-hacker-stehlen-kundendaten-von-deutscher-hotelkette-2310-178139.html
https://www.netzwelt.de/news/223190-hackerangriff-motel-one-daten-millionen-gaesten-darknet-einsehbar0910.html
https://www.tagesschau.de/wirtschaft/unternehmen/motel-one-hackerangriff-100.html

III. NCSC warns of impersonation attacks on the gamer community and new fake sextortions

A similar, albeit not quite as sophisticated, attack pattern is shown by attacks in the gamer community, which the National Cyber Security Center NSCS warned of on its website in week 40: victims are members of Discord, a platform through which gamers exchange and network. From a compromised Discord account, friends of the legitimate account owner receive an invitation to test and download a new game. If the unsuspecting victim loads the game onto their device via an Exec file, the malware comes with it. It can intercept passwords and send them to the cyber criminals. Once this has happened, they try to take control of the device and all services controlled by it. The malware attack was detected because warning messages indicated attempts to change accounts, which failed especially in those cases where the accounts were protected by 2-factor authentication.

So-called fake sextortion attacks work less with the prospect of a new computer game than with shame and fear: In mass e-mails, cyber criminals claim that they have photos or videos showing the recipient of the e-mail during an alleged visit to pornographic websites. They then threaten to publish the image or video material if the demanded ransom payment is not paid within a certain period of time. In order to underline the truthfulness of their fake claims, sextortion attackers often used the email addresses of the people being contacted or passwords used by them that they acquire for sending on the darknet. If these passwords are still active, the cybercriminals then hack into the social media accounts of the victims and explicitly upload the content there in order to block the accounts and thus make them feel insecure.

While it was previously possible to assume that the threats presented in the e-mails were built up without substance, the NCSC reports in week 39 of a case in which a screenshot of the victim's PC desk and data on the operating system used by the PC were attached to the sextortion e-mail. According to the NCSC, it has not yet been possible to determine where the screenshot and data came from, but the authority writes: "In the latest form, it can no longer be ruled out that malware has really crept onto the computer. This is because the attackers present a recent screenshot of the victim's computer as evidence."

Bleepingcomputer.com reported on an even more sophisticated new variant of fake sextortion at the beginning of September: similar to the hospitality attackers in the second article of this security report, the criminals use the fake variant of a well-known website to cash in on their victims. At "info@youporn.com", they send a deceptively real-looking message to unsuspecting victims that a video has just been uploaded showing the victim performing sexual acts. Because the security and privacy of users is taken very seriously, such videos are first filtered out to check whether the victim agrees to the publication. In this case, nothing has to be done. However, if the victim wanted the video not to be uploaded, he or she should follow a link that leads to a fake YouPorn page. There, the victim then has the option of choosing between three supposed

service plans with different - brazen! - security levels, which are offered at prices of 199, 699 and 1,399 US dollars respectively and can be paid into two Bitcoin accounts. So far, according to bleepingcomputer.com, the action has been unsuccessful, but it cannot be ruled out that further attacks will be carried out in a similar way in the future.

Read more at:

https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2023/wochenrueckblick_40.html
https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2023/wochenrueckblick_39.html
https://www.bleepingcomputer.com/news/security/fake-youporn-extortion-scam-threatens-to-leak-your-sex-tape/

IV. Ransomware - a growth market!

While the growth engines of the legal economies have noticeably stuttered in recent months, the market for ransomware seems to know no bounds. At least that is what can be concluded from the Ransomware Weekly Report on bleepingcomputer.com of 13 October 2023. Author Lawrence Abrams reported that the dreaded cybercrime group BianLian has claimed responsibility for the attack on the airline Air Canada. The APLHV group, mentioned here several times before, has attacked a number of courts in Northwest Florida. And with Simpson Manufacturing, one of the largest manufacturers of structural fasteners in the US was forced to shut down and reboot all IT systems after a cyberattack. Abrams stresses that in this case it is not clear whether the attack was an extortion attempt or an act of pure sabotage.

With 1,420 cases, cyber extortionists in the third quarter of 2023 have once again exceeded their record of 1,386 cases from the second quarter of 2023. In addition to these figures, the "Ransomware Trends Q3 2023" report by the security company cyberint (linked below) shows in a well-compiled overview that, in addition to the "industry giants" such as Lockbit3, ALPHV and BianLian, successful newcomers such as Clop were primarily active in the western industrialised nations. With 616 successful attacks, the USA was the target in almost half of all cases. The United Kingdom, Canada, Germany and France followed by a wide margin. Interestingly, the attacks were primarily focused on suppliers and business service providers, followed by industrial manufacturers and retailers. And even if Switzerland is not among the top 10 countries attacked - which is not desirable for once - Lockbit3, ALPHV, Clop and BianLian are also active as attacker groups here.

In view of the outlook in the cyberint report, this does not bode well for the legal world: New groups such as the Rhysida Ransomware Group, 3AM or Clop are not competing with the "veterans" such as Lockbit3 or ALPHV but are simply expanding the field of attack. Investing in cyber security and awareness is therefore certainly a cost-efficient way of spending money and resources for Swiss institutions and companies.

Read more at:

https://www.bleepingcomputer.com/news/security/simpson-manufacturing-shuts-down-it-systems-after-cyberattack

https://cyberint.com/blog/research/ransomware-trends-q3-2023-report

V. On our own account: Further developing the SWITCH Security Report

We are very pleased that you are among the readership of the Security Report. Your opinion will help us determine the direction in which we are going to develop this information product. Please take one minute to answer four questions.

This link will take you directly to the survey.

Thank you for taking part.

This SWITCH Security Report was written by Dieter Brecheis and Michael Fuchs.