SWITCH Security Report on the latest IT security and privacy trends

January/February 2023

SWITCH

I. A real threat to virtual machines: global attack on VMware-ESXi – patch now!

A new trend seems to be developing amongst cybercriminals: take a vulnerability that has been known for some time, assume that it has not been fixed on many devices regardless of whether patches are available or not, and exploit it mercilessly. What worked fine with Microsoft Exchange servers in the interests of the hackers now applies to VMware. In early February, the Italian cybersecurity authority ACN reported that thousands of servers around the world had been successfully attacked and infected with ransomware. Bleepingcomputer.com reported more than 3,200 infected servers. France was the hardest hit, followed by the United States, Germany, Canada and the United Kingdom. Finnish and Italian servers were also compromised. The U.S. cybersecurity agency CISA confirmed the attacks, as did the French CERT, which issued a warning shortly after the Italian authorities of massive attacks against the long-known VMware ESXi vulnerability known as CVE-2021-21974. With a CVSS value of 8.8 – as per the Common Vulnerability Scoring System – reaching up to 10.0, this gap is considered risky. It occurs in ESXi versions 7.x

(older than ESXi70U1c-17325551), 6.7x (older than ESXi670–202102401-SG) and 6.5x (older than ESXi650–202102101-SG).

Although security updates have been available since February 2021, it appears that many servers have not yet been patched despite the high risk. The French CERT therefore strongly recommends installing the patches on its website, but also points out that closing the security loophole is not, of course, sufficient if a server has already been attacked.

In the meantime, heise.de has reported that the US security agency CISA has provided recover.sh, a Unix shell script for recovering affected machines on GitHub in the ESXIArgs-Recover project. The link is provided below.

Read more at:

https://www.heise.de/news/Italiens-Cyber-Sicherheitsbehoerde-warnt-vor-weltweitem-Ransomware-Angriff-7485377.html.
https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide.
https://techcrunch.com/2023/02/06/hackers-vmware-esxi-ransomware/.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/.
https://www.heise.de/news/Ransomware-Attacke-CISA-veroeffentlicht-Wiederherstellungsskript-fuer-VMware-ESXi-7488498.html.
https://github.com/cisagov/ESXiArgs-Recover.

II. From FA to 2FA – protect your Facebook account with two-factor authentication

Despite increasingly becoming standard practice with e-banking or when logging into particularly sensitive pages, such as online accounts with health insurers, two-factor authentication is still the exception when it comes to social media accounts. Many users wonder if the effort involved in logging into their accounts is over the top. Obviously, it isn't, because even if the account content doesn't offer hackers rewarding options for exploitation in most cases, the account can be highly attractive even to cybercriminals, for example, to spread child pornography via hacked Facebook accounts.

This is precisely what the State Criminal Office of the German Federal State of Lower Saxony has pointed out. The northern German investigators have only recently observed this phenomenon and refer to it as 'Facebook hacking' or 'Facebook phishing'. First, the criminals steal the login details to the accounts – usually via phishing or by trying out widely used passwords (credential stuffing). Then they take over their victims' accounts and upload their disgraceful material.

Victims are harmed at least twice: firstly, because Facebook's parent company Meta immediately blocks the account for illegal child pornography and reports the incident to the National Center for Missing & Exploited Children NCMEC. As a quasi-governmental

U.S. agency, the NCMEC immediately relays criminal information to U.S. law enforcement agencies. If the user accounts are registered outside the US, the relevant authorities in the country concerned are informed. And there – and this is the second damage with often more far-reaching consequences – account holders are charged in criminal proceedings for possession or distribution of child or youth pornography. Admittedly, the State Criminal Office of Lower Saxony points out in its report that the German public prosecutors will in most cases close the proceedings as soon as it is ascertained that the account had been hacked. However, the procedure is certainly not pleasant for those affected.

If you want to protect yourself against this, Facebook has been able to generate a TOTP (Time-based One-Time Password) or offer (not so good) two-factor authentication via SMS for some time now. You can find out how to do this in the help section on facebook.com. However, it became known at the end of January that a vulnerability in both Facebook and its sister medium Instagram allowed two-factor authentication via SMS to be bypassed. The Zuckerberg Group has confirmed the vulnerability and paid its discoverer 27,000 dollars from its in-house bug bounty programme. However, it is not yet known whether the gap has been closed since then.

Read more at:

https://www.heise.de/news/LKA-Warnung-Kinderpornografie-Posts-nach-Facebook-Hacks-7487612.html.
https://www.golem.de/news/2fa-wie-sicher-sind-totp-fido-sms-und-push-apps-2206-166287-3.html.
https://www.facebook.com/help/358336074294704.
https://www.heise.de/news/Zwei-Faktor-Authentifizierung-Facebook-Instagram-Bug-ermoeglichte-Umgehung-7476725.html.

III. AI breaking bad – how cybercriminals use chatGPT and other artificial intelligence

In a t3n portrait, Open AI CEO Sam Altmann is quoted as saying: 'I am particularly concerned that it (the AI application, editor's note) is accidentally misused.' On this point, the man behind ChatGPT can be reassured. AI applications are misused, but not accidentally, rather deliberately. And on an ever-increasing scale.

Several security blogs addressed the issue at the end of January. Amongst other things, the well-known cybersecurity company McAfee posted a blog post on 25 January that explicitly warns against hackers exploiting the undoubtedly enormous capabilities of AI ChatGPT in several ways.

On the one hand, they could take malware to new dimensions, both quantitatively and qualitatively, because ChatGPT does not need to take any breaks and can write malware 24/7 and around the clock. Worse still, ChatGPT and other highly developed AI are capable

of developing what is known as polymorphic malware, which evolves on a quasi-self-learning basis and is therefore virtually impossible to find, let alone combat.

On the other hand, ChatGPT, acting like a Cyrano de Bergerac of the 22nd Century, could tempt naive users to send sensitive personal data or money on dating platforms using unlimited and perfectly formulated pledges of love through fake profiles.

Speaking of perfectly formulated: while phishing e-mails could often be identified simply by incorrect spelling or grammar, this becomes almost impossible when hackers accidentally use the services of ChatGPT – although one might ask which is bigger: the spelling and grammar gaps of North Korean phishers or the (perhaps even deliberately staged as a distraction?) naivety of a Sam Altman. In addition to ChatGPT, his company provides the basis for AI-based creation of phantom images with the artificial intelligence DALL-E. Criticism is not only directed at the fact that these images are based on far less complex criteria than would be the case in the case of testimonies based on human memories. Rather, DALL-E itself is accused of being heavily prejudiced. According to reports by futurezone.at, AI only generated images of white men after entering the acronym 'CEO,' whereas images of dark-skinned men and Latinos were generated after entering the acronym 'Gangster' and images of women always appeared on the output screens.

Nevertheless, all tech giants see AI as the 'next big thing'. Now that Microsoft has integrated ChatGPT into its search engine BING, it's hardly surprising that Google has announced its own offer with 'Bard' to defend its search engine position and open up new opportunities. It will be interesting to see whether the Cola Wars of the 1990s will find their modern continuation in the AI battles of the 22nd century.

Read more at:

https://t3n.de/news/sam-altmann-der-mann-hinter-chatgpt-open-ai-1530670.
https://securityaffairs.com/140380/hacking/hackers-exploiting-chatgpt.html.
https://www.mcafee.com/blogs/internet-security/chatgpt-a-scammers-newest-tool/.
https://cyberscoop.com/chatgpt-ai-malware/.
https://futurezone.at/digital-life/ki-phantombilder-phantomzeichnungen-polizei-zeugen-kuenstliche-intelligent-dall-e-openai/402321494.
https://futurezone.at/science/bildgenerator-kuenstliche-intelligenz-dall-e-imagen-google-artificial-intelligence/402050017.
https://www.indiatimes.com/technology/news/ai-programme-generates-police-sketches-of-potential-suspects-592537.html.
https://www.handelszeitung.ch/tech/chat-gpt-open-ai-und-microsoft-starten-offensive-gegen-google-571387.
https://www.hackread.com/google-bard-chatgpt-rival/.

IV. Cyber extortionist in the red = cyber attacks in the black

Profits from ransomeware attacks are expected to have plummeted by 40% in 2022, according to statistics published at the end of January by the blockchain platform 'chainalysis'. At the same time, it points to a disproportionately higher undeclared

number. How high this actually must be can be deduced from the fact that, according to internal UN reports, the North Korean state cyber criminals of the global blackmailer Kim Jong-Un alone would have generated record revenues of around USD 1.2 billion in 2022.

By contrast, the chainalysis statistics show a total 'return' of all officially known ransomware revenues for 2022 of USD 457 million, compared with USD 766 million in 2021 – a drop of USD 309 million. Around 130 million dollars of this can be explained by the takedown of HIVE alone. This network of cybercriminals, which has been active internationally since 2021, specialised in ransomware-as-a-service. It has been blamed for attacks on more than 1,500 victims with damages of more than 100 million dollars.

In an internationally coordinated undercover campaign, investigative teams led by the FBI together with German and Dutch investigators have infiltrated the HIVE network since 2022. They pulled over 300 decryption codes and passed them on to attacked victims. This allowed them to decrypt their devices and refuse ransom demands demanded by HIVE. In addition, the investigators secured about 1,000 additional decryption keys from previous attacks.

bleepingcomputer.com also reports that more and more victims of attacks do not comply with the demands for payment of a ransom, citing statistics from the cybersecurity company Coveware. According to them, for the first time in 2022, the proportion of those who refused to pay a ransom was greater than those who paid. While this ratio was 24% to 76% in 2019, it dropped to 59% to 41% in 2022.

Unfortunately (though to be expected), cyber gangsters are reacting to this annoying development by changing their business models in various directions. Firstly, they increase the ransom demands in order to squeeze more money out of their victims. Secondly, they don't just attack their victims with one specific ransomware (such as Cryptolocker, Petya, Bad Rabbit, etc.), but rather use several ransomware strains at the same time. In addition, they are attacking victims who have already paid before. Coveware notes that this strategy used to target small companies and organisations, but is now also being used against medium-sized companies and large players.

It has also been observed that some groups are changing the blackmail process themselves. While double pay day criminals demand a second ransom after the first ransom payment for decrypting the data so that the data is then not published, in some recent ransomware attacks hackers have skipped the encryption part of an attack, instead focusing on stealing the data and threatening to publish it. This makes attacks easier and faster, giving attackers more security against detection and tracking. It also increases the likelihood that organisations of critical infrastructures will pay because they want (or have) to prevent sensitive data from reaching the public.

Read more at:

https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay
https://www.stern.de/digital/un-bericht--un--nordkoreas-hacker-stehlen-rekordsummen---kim-ruestet-auf-33172534.html
https://www.zdnet.com/article/doj-takes-down-ransomware-group-with-a-21st-century-cyber-stakeout
https://www.bleepingcomputer.com/news/security/ransomware-profits-drop-40-percent-in-2022-as-victims-refuse-to-pay
https://www.darkreading.com/attacks-breaches/ransomware-profits-decline-victims-refuse-pay

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.