SWITCH Security Report on the latest IT security and privacy trends

July/August 2023

SWITCH

I. Are jet-black clouds gathering instead of an azure-blue sky? Microsoft Azure master key theft

Is it a disaster or a 'straightforward' hack? In mid-June, US authorities informed Microsoft of suspicious access to e-mails in their MS Exchange accounts. The analysis revealed that a signature key to Microsoft's cloud services had been stolen and used by the hackers to gain access to data, primarily from European and US authorities.

Microsoft initially stated that Chinese cybercriminals had got hold of an inactive MSA key and its signatures were intended only for private customers. However, 'validation issues' had led to the signatures created with the key being recognised by Azure's Active Directories for business customers.

At the end of July, the security company WiZ reported that the stolen key was by no means simply any old key. Rather, it is an OpenID signing key for the Azure Active Directory. As a result, virtually all users of Microsoft's cloud services are exposed to the risk of cybercriminals gaining access to their networks, devices or data via Outlook, SharePoint, Office 365, Teams, OneDrive or other applications that offer 'Sign in with Microsoft'. Microsoft locked the

compromised key, but cybercriminals would have had enough time to use it to set up back doors in virtually the entire Microsoft cloud.

Bruce Schneier reported that they have already done so in his blog 'Schneier on Security' on 7 August. The victims of the attacks included several American government agency networks. When comparing with previous SolarWinds attacks by Russian cybercriminals, he points out that more than 14,000 networks around the world experienced attacks at that time. He also adds that although their operators patched them, the cybercriminals installed backdoors in the meantime and are now almost impossible to get out of the networks. His observation that cybercriminals around the world were focussing on attacking infrastructure providers instead of the well-protected organisations themselves was confirmed by the Xplain hack in Switzerland. The Azure master key theft also demonstrates the same pattern.

In response to customers' dissatisfaction with Microsoft's handling of the case, it was announced after a few days that the login process for cloud services had been refined and improved and that the roll-out of updates would begin in September. Amit Yoran, CEO and Chairman of cybersecurity company Tenable, complained about the lack of transparency and claimed that due to this, Microsoft is putting the credibility of cloud services at risk in an article published on LinkedIn, which is ironically owned by Microsoft.

On 4 August, heise.de then reported that Microsoft had published a playbook, which Azure users could use to see whether their organisation is affected by the Azure hack, whether backdoors have been installed and whether access to the network has been compromised. The 'Token Theft Playbook' is available in English and German as a playbook for data theft and can be downloaded via the link below.

Read more at:

https://www.heise.de/news/Gestohlener-Cloud-Master-Key-Microsoft-schweigt-so-fragen-Sie-selber-9229395.html
https://www.schneier.com/blog/archives/2023/08/microsoft-signing-key-stolen-by-chinese.html
https://www.heise.de/news/Neue-Erkenntnisse-Microsofts-Cloud-Luecken-viel-groesser-als-angenommen-9224640.html
https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access
https://www.microsoft.com/en-us/security/blog/2023/07/19/expanding-cloud-logging-to-give-customers-deeper-security-visibility
https://www.linkedin.com/pulse/microsoftthe-truth-even-worse-than-you-think-amit-yoran
https://www.heise.de/news/Nach-dem-geklauten-Master-Key-fuer-Azure-Hilfestellung-von-Microsoft-9234954.html
https://learn.microsoft.com/en-us/security/operations/token-theft-playbook
https://learn.microsoft.com/de-de/security/operations/token-theft-playbook

II. Microsoft in a blizzard: Russian state hacking group Midnight Blizzard using Teams to phish

In contrast with the Azure disaster, Microsoft acted proactively in a different case. On 3 August, the tech giant headquartered in Redmond warned that a Russian hacking group was attempting to phish login details from MS Teams users. The cybercriminals, known as ATP29,

Nobelium and now Midnight Blizzard, are claimed to be Russian state actors and accused of espionage by the US and British authorities.

The current wave of social engineering attacks is much more sophisticated than the well-known telephone phishing attempts, in which cybercriminals pretend to be Microsoft support in that they focus on small and very small companies that they have already compromised in previous attacks. They rename a person employed there, add a new onmicrosoft.com subdomain, and send an outgoing message via Teams to target users in global organisations under the new domain. In these cases, they pretend to be Microsoft support and try to persuade the victim to hand over multi-factor authentication data in chats.

According to Microsoft, 40 government organisations, NGOs and companies from the fields of discrete manufacturing, IT, media and technology have been the victims of such attacks to date. Microsoft therefore recommends continuously raising users' awareness of security issues and treating authentication requests that were not initiated directly by users as malicious.

Read more at:

https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams
https://www.bleepingcomputer.com/news/security/russian-hackers-target-govt-orgs-in-microsoft-teams-phishing-attacks
https://www.heise.de/news/Midnight-Blizzard-Microsoft-warnt-vor-Hackern-die-Anmeldedaten-erbeuten-wollen-9233919.html
https://securityaffairs.com/149103/apt/apt29-microsoft-teams-phishing-attacks.html

III. LinkedIn: enable two-factor authentication before cybercriminals do so

In a blog post in mid-August, cybersecurity company Cyberint drew attention to the massive increase in attacks on accounts in the LinkedIn business network. Cybercriminals would try to use brute force attacks to obtain members' login details or simply delete the account. It is therefore advisable to reset your password and enable two-factor authentication – even if this could potentially lead to LinkedIn blocking your account temporarily if an attack is detected. In this case, LinkedIn will then prompt the affected person to verify their account and create a new password. The account will then be unblocked again.

Both measures are sensible simply because, following a cyber-attack on LinkedIn two years ago, the data of 700 million users was put up for sale on the dark net. Cybercriminals are now apparently also using this data to log into unprotected accounts, then change passwords and activate two-factor authentication in order to lock out real users.

The company has compiled all answers and to-dos in a post (linked below) on the LinkedIn help page. These are both for the event that members are still able to open their account but suspect misuse, as well as for the event that they are no longer able to access their own account despite using the valid login details.

Read more at:

https://cyberint.com/blog/research/linkedin-accounts-under-attack-how-to-protect-yourself
https://www.golem.de/news/jetzt-2fa-aktivieren-hackerangriffe-auf-linkedin-konten-nehmen-massiv-zu-2308-176794.html
https://www.businessinsider.de/wirtschaft/verbraucher/cyber-angriff-auf-linkedin-fast-jeder-nutzer-ist-betroffen/
https://www.linkedin.com/help/linkedin/answer/a1340402

IV. Can AI dial into Zoom meetings?

According to the company, the coronavirus pandemic made Zoom the market leader for stand-alone video conferencing software. While there were 'only' 10 million active monthly users in 2019, this figure soared to 200 million in March 2020. The market value and profits of the company, which was founded in San José in 2011, also increased at a similar rate. In March, the provider then amended its General Terms and Conditions to enable it to record data from the recorded conferences for training purposes. However, Zoom didn't want to train its own employees, but rather artificial intelligence.

According to the Chaos Computer Club Zürich, Zoom has since stored poll results, pictures, chat content and presentation material for training AI without informing users, let alone obtaining their consent. This data use, which is protected by the new GTCs, became public only thanks to a publication from stackdiary.com on 6 August. The ensuing wave of protests spread virally and not only pushed down the company's stock market price noticeably, it also brought with it an initial change to Zoom's GTCs the very next day, in which the video conferencing service promised to use data only with users' consent.

However, the wave continued, meaning Zoom founder and CEO Eric Yuan was forced to U-turn after completing stopping the plan and publish revised GTCs on 11 August, in which Zoom rules out any use of conference data to train both its own and third-party AI: "Zoom does not use any of your audio, video, chat, screen sharing, attachments or other communications-like Customer Content (such as poll results, whiteboard and reactions) to train Zoom or third-party artificial intelligence models."

Read more at:

https://www.beobachter.ch/digital/zoom-verwendet-nutzerdaten-fur-ki-trainings-628402
https://march24.ch/articles/202564-zoom-nutzt-userdaten-zum-training-von-ki
https://www.inside-it.ch/zoom-will-userdaten-fuers-ki-training-nutzen-20230808
https://stackdiary.com/zoom-terms-now-allow-training-ai-on-user-content-with-no-opt-out
https://www.zeit.de/digital/datenschutz/2023-08/datenschutz-videokonferenz-zoom-nutzerdaten-kuenstliche-intelligenz-ki-training
https://www.handelszeitung.ch/newsticker/zoom-datennutzung-zum-ki-training-nur-mit-zustimmung-der-nutzer-626368
https://www.finanzen.ch/nachrichten/aktien/nach-heftiger-empoerung-zoom-rudert-bei-datennutzung-fuer-ki-training-zurueck-1032571838

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 Frank Herberg.

The SWITCH Security Report does not reflect the opinion of SWITCH. Rather, it is a compilation of various media reports. SWITCH assumes no liability whatsoever for the content and opinions set out in the Security Report or their accuracy.