Notes sur l'utilisation du service de visioconférence Zoom
++

Articles sur le sujet
=====================

-> 10/10/2020
-> Zoom aurait menti aux utilisateurs sur le chiffrement de bout en bout pendant des années, Selon une plainte de la FTC
    => Le 10 novembre 2020 à 10:10, par Bill Fassinou
    => https://www.developpez.com/actu/310313/Zoom-aurait-menti-aux-utilisateurs-sur-le-chiffrement-de-bout-en-bout-pendant-des-annees-selon-une-plainte-de-la-FTC/
    => Sources : FTC, Plainte de la FTC (PDF)
        => https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement
        => https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint.pdf
--
Zoom, le service de visioconférence qui a vu sa cote de popularité explosée avec la pandémie du Covid-19, fait face à de nouvelles allégations en matière de sécurité. Dans une plainte ce 9 novembre, la FTC (Federal Trade Commission) a accusé la société d'avoir trompé les utilisateurs sur le niveau de sécurité de la plateforme de réunion Zoom et a également injustement sapé une fonction de sécurité du navigateur Safari d'Apple. Zoom avait annoncé mi-octobre qu'il allait commencer à proposer le chiffrement de bout en bout sous forme de Technical Preview.

Zoom est l’un des grands bénéficiaires de cette pandémie : il a connu une hausse de son utilisation, en passant de 10 millions en décembre 2019 à 300 millions d'utilisateurs actifs par jour en avril 2020. Le revers de la médaille a été une attention particulière portée à l’application, notamment par les experts en sécurité et les régulateurs, dont la FTC. Ainsi, dès le mois de mars 2020, des bogues ont été relevés dans l'application et il a aussi été découvert que les réunions Zoom ne supportaient pas le chiffrement de bout en bout, ce qui donne la possibilité à l'entreprise d'espionner les réunions vidéo privées.
--

-> 15/10/2020
-> Zoom annonce qu'il va proposer le chiffrement de bout en bout sous forme de Technical Preview la semaine prochaine
    -> Pour les clients de la version gratuite et payante
    => Le 15 octobre 2020 à 14:06, par Stéphane le calme
    => https://www.developpez.com/actu/309692/Zoom-annonce-qu-il-va-proposer-le-chiffrement-de-bout-en-bout-sous-forme-de-Technical-Preview-la-semaine-prochaine-pour-les-clients-de-la-version-gratuite-et-payante/
--
Zoom a été l’un des grands bénéficiaires de cette pandémie : le service de visioconférence a vu son pic d’utilisation exploser au point de franchir la barre des 300 millions journaliers d’utilisateurs. Le revers de la médaille a été une attention particulière portée à l’application, notamment par des experts en sécurité. C’est dans ce contexte que des bogues ont été découverts, mais aussi le fait que les réunions Zoom ne supportaient pas le chiffrement de bout en bout.

Dans le livre blanc de Zoom, il existe une liste de « fonctionnalités de sécurité avant la réunion » disponibles pour l'hôte de la réunion qui commence par « Activer une réunion chiffrée de bout en bout (E2E) ». Plus loin dans le livre blanc, il est fait mention de « Sécuriser une réunion avec le chiffrement E2E » comme étant une « capacité de sécurité en réunion » disponible pour les hôtes de réunion. Lorsqu'un hôte démarre une réunion avec le paramètre « Exiger le chiffrement pour les points de terminaison tiers » activé, les participants voient un cadenas vert qui dit, « Zoom utilise une connexion chiffrée de bout en bout » lorsqu'ils passent la souris dessus.

Mais lorsque l’entreprise a été contactée pour savoir si les réunions vidéo sont réellement chiffrées de bout en bout, un porte-parole de Zoom a écrit : « Actuellement, il n'est pas possible d'activer le chiffrement E2E pour les réunions

vidéo Zoom. Les réunions vidéo Zoom utilisent une combinaison de TCP et UDP. Les connexions TCP sont établies à l'aide de TLS et les connexions UDP sont chiffrées avec AES à l'aide d'une clé négociée sur une connexion TLS ».

Face à la réaction que cela a provoqué, l'entreprise a décidé de travailler sur ces points de sécurité. L'entreprise a d'abord rappelé que son offre était destinée principalement aux entreprises ; elle n'avait donc pas anticipé la popularité soudaine au sein des utilisateurs personnels.
--
Voir aussi l'article du 31/03/2020 => https://mobiles.developpez.com/actu/298743/Les-reunions-sur-Zoom-ne-supportent-pas-le-chiffrement-de-bout-en-bout-Zoom-a-donc-la-capacite-technique-d-espionner-les-reunions-video-privees/

-> 07/07/2020
-> La plupart des services de visioconférence ne sont pas conformes au RGPD
    => 07/07/2020 à 07h25 - Gilbert KALLENBORN - Journaliste
    => https://www.01net.com/actualites/la-plupart-des-services-de-visioconference-ne-sont-pas-conformes-au-rgpd-1943911.html
    => Source: datenschutz-berlin.de => https://www.datenschutz-berlin.de/infothek-und-service/pressemitteilungen/
--
Teams, Zoom, Meet… Les grandes marques de visioconférence épinglées par une autorité de protection des données personnelles allemande.

Les services de visioconférence se sont révélés fort pratiques durant cette crise de coronavirus, mais sont-ils conformes à la protection européenne de données personnelles ? La réponse est non, a estimé l'autorité de protection des données personnelles de Berlin. Celle-ci a analysé les conditions d'utilisation de 17 services professionnels. Seuls cinq ont trouvé grâce à ses yeux et obtenu un « feu vert » dans leur tableau : Wire, Tixeo, sichere-videokonferenz.de, Jitsi-Netways et Werk21. Les grandes marques – telles que Microsoft Teams, Google Meet, Skype ou Zoom – ont récolté un « feu rouge » signalisant des contrats de traitement de données non conformes aux textes de loi.

Dans les conditions de Microsoft Teams, l'autorité a noté des « contradictions », un « manque de clarté » et des « exportations de données illicites ». Celles de Zoom et de Google Meet ne respecteraient pas, entre autres, le droit à l'effacement des données. Au final, l'autorité recommande aux entreprises de ne pas utiliser ces services et de se restreindre aux cinq services qui respectent les règles, du moins formellement.
--

-> 19/06/2020
-> Zoom Offers Encryption To All
    => By David Roe | Jun 19, 2020
    => https://www.cmswire.com/digital-workplace/zoom-offers-encryption-to-all-basecamp-releases-email-platform-and-more-news/
--
Sometimes when you look at San Francisco-based video conferencing platform Zoom and the problems it has been having over the past few weeks, particularly in respect of security, you really get the impression that it's biggest problem is public relations. Over the past few weeks, its CEO, Eric Yuan, undertook what might be described as a charm offensive while at the same time offering concrete solutions to widely held concerns about the security of its video meetings.

However, despite assuring users that encryption was on the way, when the announcement finally came it created outrage. Encryption, he said, was available, but only for paying customers. The reactions were predictable. On a call with analysts and cited in many news outlets he said: "Free users for sure we don't want to give [end-to-end encryption] because we also want to work together with FBI, with local law enforcement in case some people use Zoom for a bad purpose."

With millions of people around the world working remotely and using Zoom the announcement was poorly received. "In an online world, encryption is paramount to privacy, and privacy promotes safety, liberty and fairness into our social fabric. Gating personal privacy behind a paywall erodes basic freedoms and fairness, shared Tim Wade, technical director at the cybersecurity firm Vectra, in the

Guardian newspaper.

Little surprise, then, that Zoom backed down. In a blog post in the middle of this week, Juan did an about-turn and wrote that everyone will get the new encryption. Changes he made to the E2EE (End-to-End-Encryption) design that were published on GitHub will enable the company “to offer E2EE as an advanced add-on feature for all of our users around the globe – free and paid – while maintaining the ability to prevent and fight abuse on our platform.”

There will be a new process for users signing up but nothing more than is expected for many two-step login processes with other apps.leading companies perform similar steps on account creation to reduce the mass creation of abusive accounts.

For now though, things stay the way they are with Zoom planning to introduce the early beta of the E2EE feature in July 2020. “We are grateful to those who have provided their input on our E2EE design, both technical and philosophical. We encourage everyone to continue to share their views throughout this complex, ongoing process,” Juan added.

The video platform exploded in popularity after coronavirus-related lockdowns and is now seeing as many as 300 million daily users, up from just 10 million in December.
--

-> 03/06/2020
-> Fil twitter de Nico Grant @NicoAGrant
    => 5:25 AM · 3 juin 2020
    => https://twitter.com/NicoAGrant/status/1268020841054269440
--
Zoom’s CEO says he won’t encrypt free calls so Zoom can work more with law enforcement:
“Free users for sure we don’t want to give that because we also want to work together with FBI, with local law enforcement in case some people use Zoom for a bad purpose,” Yuan said. $ZM
--
Pouet sur Mastoton:
-> nothing2hide -> @nothing2hide@mamot.fr
    => 03 juin 2020 à 07:50 ·
--
Le président de @zoom_us@twitter.com déclare que sa société ne chiffrera pas les appels vidéos passés avec des comptes gratuits afin de pouvoir coopérer avec les forces de l’ordre.
N’UTILISEZ PAS ZOOM.
--

-> 20/05/2020
-> "Maintenant vous savez"
-> Qu'est-ce qu'un webinaire ? Merci d'avoir posé la question !
    => https://play.acast.com/s/maintenant-vous-savez/qu-estcequ-unwebinaire-
    => by Bababam => https://play.acast.com/s/maintenant-vous-savez
    => On y parle de Zoom et des problèmes qu'elle pose en terme de vie privée !...
--
"Webinaire" est la contraction des mots web et séminaire pour qualifier toute forme de réunion interactive de type séminaire en ligne, appelé communément visio-conférence. Certains webinaires sont réalisés dans un usage interne des organisations comme des réunions, des formations ou certaines discussions, tandis que d’autres sont adressés à l'extérieur pour une audience plus large. Les plateformes qui le permettent éliminent ainsi les contraintes liées au déplacement, au coût et à la logistique. Favorisant une mise en réseau interactive, rapide et simple d’utilisation.

Pourquoi n'a-t-on jamais autant parlé du webinaire qu'aujourd'hui ?

Depuis le début du confinement et la mise en place du télétravail dans certaines entreprises, l’utilisation des webinaires pour organiser le quotidien a explosé. Les professeurs ont dû également réagir dans l’urgence pour assurer la continuité pédagogique. Et même Pôle Emploi s’y met pour proposer des formations à

destination des demandeurs d’emploi et mettre ainsi à profit ce temps de confinement.

Se former, collaborer, produire, mettre en réseau ou fêter des anniversaires, les objectifs sont aussi différents que les utilisateurs des webinaires. La mise en place du confinement sans préavis a pris tout le monde de court.

Quelles sont les plateformes qui permettent des webinaires ? Nos données personnelles sont-elles protégées ? Quelles sont les alternatives aux grosses plateformes pour mieux nous protéger ? Toutes les réponses sont dans cet épisode de "Maintenant vous savez".
--
Podcast (4'33") => https://sphinx.acast.com/maintenant-vous-savez/qu-estcequ-unwebinaire-/media.mp3

-> 11/05/2020
-> Zoom Settles with NY AG Over COVID-19-Related Privacy, Security Issues
    => https://healthitsecurity.com/news/zoom-settles-with-ny-ag-over-covid-19-related-privacy-security-issues
    => By Jessica Davis - May 11, 2020 - En anglais !
--
As COVID-19 drove Zoom participation up 2,000 percent, reports found serious privacy and security risks in the platform; the New York AG settlement will enforce security controls requirements.
Zoom settled with New York Attorney General Letitia James on May 7, following a state-led investigation into the videoconferencing platform. James launched an investigation after a number of privacy and security failings were brought to light by the spike in Zoom participants amid the COVID-19 pandemic.
--
Alors que COVID-19 a fait grimper la participation de Zoom de 2 000%, les rapports ont révélé de sérieux risques de confidentialité et de sécurité sur la plate-forme; le règlement de New York AG imposera des exigences en matière de contrôles de sécurité.
Zoom s'est installé avec le procureur général de New York, Letitia James, le 7 mai, à la suite d'une enquête menée par l'État sur la plate-forme de vidéoconférence. James a lancé une enquête après qu'un certain nombre de manquements à la vie privée et à la sécurité ont été révélés par la montée en flèche des participants à Zoom au milieu de la pandémie de COVID-19.
--

-> 08/05/2020
-> Zoom Buys Encryption Provider Keybase
    => By David Roe | May 8, 2020
    => https://www.cmswire.com/digital-workplace/zoom-buys-encryption-provider-keybase-google-offers-meet-to-gmail-users-more-news/
--
This week, we turn yet again to the videoconferencing market and the jostling among vendors for supremacy as millions of workers are forced to work remotely. While there have been numerous contenders for the "most popular" video app title, Zoom's profile has grown more than Microsoft Teams, for example, which is restricted to Microsoft environments. However, Zoom has become as widely known for its problems as it has for its benefits.

One of those problems has been security and its lack of end-to-end encryption. Even with all the talent in the world, it would be impossible to develop end-to-end encryption in the 90-day "fix" period that CEO Eric Yuan has given the company to sort out its problems.

To solve the problem, he announced that Zoom is buying Keybase, a company that has built a secure messaging and file sharing service using its deep encryption and security expertise. According to a statement from Yuan, Zoom will integrate Keybase’s entire team into Zoom and use that team to build end-to-end encryption that can be applied to Zoom services now and as it scales up in the future.

“This acquisition marks a key step for Zoom as we attempt to accomplish the creation of a truly private video communications platform, Yuan wrote. “Our goal is to provide the most privacy possible for every use case, while also balancing

the needs of our users and our commitment to preventing harmful behavior on our platform."
--

-> 28/04/2020
-> What We Can Learn From Zoom's Privacy Problems
    => By David Roe | Apr 28, 2020
    => https://www.cmswire.com/information-management/what-we-can-learn-from-zooms-privacy-problems/
--
San Jose, Calif.-based Zoom is a conflicted company at the moment. While it has never had it so good in terms of the number of people using it for remote work, it is also struggling to convince those users that the privacy issues that have been revealed over the past few months are being addressed.

As part of a "charm" offensive to keep its forward momentum going, CEO Eric S. Yuan announced that he would hold weekly webinars to outline the progress the company is making in making the platform safer. The most recent one, week ending April 27th, announced the release of Zoom 5.0 and the fact that the company had reached a new milestone of 300 million daily Zoom meeting participants. With v5.0 there were two new security features introduced that are designed to safeguard people’s data:

Support for AES 256-bit GCM: Zoom 5.0 supports AES 256-bit GCM encryption, which provides more protection for meeting data and greater resistance to tampering. Organizations will have access to GCM encryption with the release of Zoom 5.0, and a system-wide account enablement will occur May 30, when all Zoom customers will switch to the new cryptographic mode.
Report a user: Hosts and co-hosts can report users to Zoom’s Trust & Safety team, who will review any potential misuse of the platform and take appropriate action. This feature will be found within the Security icon in the meeting controls.
--

-> 17/04/2020
-> Will Zoom's Never-Ending Privacy Fixes Restore User Confidence?
    => By David Roe | Apr 17, 2020
    => https://www.cmswire.com/digital-workplace/will-zooms-never-ending-privacy-fixes-restore-user-confidence/
--
For San Jose, Calif.-based Zoom, the current health crisis should have been a major opportunity to expand its reach. Millions of workers sent home to work remotely, and an entirely new audience for an app that is easy to use and, through its free plan, a way into new enterprises and new industries. The health crisis has proven difficult for the app that is now under scrutiny on both sides of the Atlantic.

Indeed, scrutiny is an understatement. Zoom now is the subject of numerous investigations into breaches of privacy, claims that it had been sending user data to Facebook and, of course, "Zoom bombing", a practice whereby uninvited guests interrupt conference calls with, in some cases, unwanted comments and even pornography. In fact, it is so bad that Google, earlier this month, banned Zoom video conferencing application from its employees’ laptops, citing security concerns. “Recently, our security team informed employees using Zoom Desktop Client that it will no longer run on corporate computers as it does not meet our security standards for apps used by our employees,” Google spokesman Jose Castaneda in a widely reported statement.
--

→ 13/04/2020
→ Over 500,000 Zoom accounts sold on hacker forums, the dark web
    ⇒ By Lawrence Abrams – April 13, 2020 – 02:05 PM – En anglais !
    ⇒ https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/
–
Over 500,000 Zoom accounts are being sold on the dark web and hacker forums for less than a penny each, and in some cases, given away for free.

These credentials are gathered through credential stuffing attacks where threat actors attempt to login to Zoom using accounts leaked in older data breaches. The successful logins are then compiled into lists that are sold to other hackers.

Some of these Zoom accounts are offered for free on hacker forums so that hackers can use them in zoom-bombing pranks and malicious activities. Others are sold for less than a penny each.

Cybersecurity intelligence firm Cyble told BleepingComputer that around April 1st, 2020, they began to see free Zoom accounts being posted on hacker forums to gain an increased reputation in the hacker community.
—
Plus de 500 000 comptes Zoom sont vendus sur le dark web et les forums de hackers pour moins d'un sou chacun, et dans certains cas, distribués gratuitement.

Ces informations d'identification sont collectées via des attaques de bourrage d'informations d'identification où les acteurs de la menace tentent de se connecter à Zoom à l'aide de comptes ayant fait l'objet d'une fuite dans d'anciennes violations de données. Les connexions réussies sont ensuite compilées dans des listes qui sont vendues à d'autres pirates.

Certains de ces comptes Zoom sont offerts gratuitement sur les forums de pirates afin que les pirates puissent les utiliser dans des farces de bombardement de zoom et des activités malveillantes. D'autres sont vendus pour moins d'un sou chacun.

La société de renseignement sur la cybersécurité Cyble a déclaré à BleepingComputer que vers le 1er avril 2020, ils ont commencé à voir des comptes Zoom gratuits publiés sur des forums de hackers pour gagner en réputation dans la communauté des hackers.
—

OU

→ 14/04/2020
→ 500 000 comptes Zoom en vente sur le darkweb
    ⇒ Nicolas Certes, publié le 14 Avril 2020
    ⇒ https://www.lemondeinformatique.fr/actualites/lire-500-000-comptes-zoom-en-vente-sur-le-darkweb-78769.html
—
Alors que les entreprises et particuliers se tournent massivement vers Zoom pendant le confinement, l'éditeur Cyble a révélé avoir trouvé sur le dark web plus de 500 000 comptes du service de visioconférences mis en vente.
—

Ou encore

→ 14/04/2020
→ Zoom : les mots de passe de 500 000 comptes piratés sont en vente sur le dark web
    ⇒ Par David Igue, 14/04/2020
    ⇒ https://www.phonandroid.com/zoom-mots-de-passe-500-000-comptes-pirates-vente-dark-web.html
—
Les adresses email, mots de passe et autres données de plus de 500 000 comptes Zoom sont en vente sur le dark web pour moins d’un cent par compte. Dans certains cas, ces informations sont rendues disponibles gratuitement.
—

Et une petite recherche vous en fournira des centaines d’autres !…
⇒ https://duckduckgo.com/?q=500+000+comptes+Zoom+pirat%C3%A9s&ia=web

Le problème étant récurrent avec Zoom, comment oser croire que le problème serait totalement réglé en cette fin juin ???

-> 06/04/2020
-> Zoom Lawsuit Brings Video Conferencing Security Into the Spotlight

    -> By Dom Nicastro | Apr 6, 2020
    => https://www.cmswire.com/digital-workplace/zoom-lawsuit-brings-video-conferencing-security-into-the-spotlight/
--
It may be the ubiquitous feel-good workplace share amid the COVID-19 health crisis: a screenshot of employee faces on a Zoom video conference call accompanied by a positive message of teamwork. But not everyone is feeling good about Zoom, though. The massive spike in usage (10 million daily users in December to 200 million now) comes with major concerns over privacy and security that has brought a class action lawsuit and the attention of federal and state regulators.

A user this week sued the video-conference provider for sharing personal information without proper notice, to third-party providers like Facebook. The New York Times reported Zoom sent user names and email addresses to a company system then matched them with LinkedIn profiles. The FBI issued warnings of “Zoom-bombing” after receiving multiple reports of hackers disrupting conferences with pornographic and/or hate images and threatening language. The New York Attorney General sent a letter to Zoom asking about its security and privacy practices.

The big questions now? How can enterprises ensure workplace apps like Zoom provide them with ever-so necessary capabilities like video-conferencing while protecting employee privacy and their organization’s sensitive information? What due diligence is required on behalf of enterprises as they navigate these applications in their (much more crowded) digital workplaces?
--

-> 31/03/2020
-> Les réunions sur Zoom ne supportent pas le chiffrement de bout en bout
    -> Zoom a donc la capacité technique d'espionner les réunions vidéo privées
    => Le 31 mars 2020 à 18:07, par Stéphane le calme
    => https://mobiles.developpez.com/actu/298743/Les-reunions-sur-Zoom-ne-supportent-pas-le-chiffrement-de-bout-en-bout-Zoom-a-donc-la-capacite-technique-d-espionner-les-reunions-video-privees/
--
Zoom, le service de visioconférence dont l'utilisation a explosé au milieu de la pandémie de Covid-19, prétend implémenter un chiffrement de bout en bout, un protocole largement compris comme la forme de communication Internet la plus privée puisqu’il protège les conversations de toutes les parties extérieures. En fait, Zoom utilise sa propre définition du terme, celle qui permet à Zoom d'accéder à la vidéo et à l'audio non chiffrés à partir des réunions.

Avec des millions de personnes dans le monde travaillant à domicile afin de ralentir la propagation du coronavirus, les affaires sont en plein essor pour Zoom, ce qui n’a pas manqué d’attirer l'attention sur l'entreprise et ses pratiques de confidentialité, y compris une politique, mise à jour plus tard, qui semblait donner à l'entreprise l'autorisation d'exploiter des messages et des fichiers partagés lors de réunions à des fins de ciblage publicitaire.
--

-> 31/03/2020
-> Zoom meetings aren’t end-to-end encrypted, despite misleading marketing
    => Micah Lee, Yael Grauer - March 31 2020, 10:00 a.m. - En anglais !
    => https://theintercept.com/2020/03/31/zoom-meeting-encryption/
--
ZOOM, THE video conferencing service whose use has spiked amid the Covid-19 pandemic, claims to implement end-to-end encryption, widely understood as the most private form of internet communication, protecting conversations from all outside parties. In fact, Zoom is using its own definition of the term, one that lets Zoom itself access unencrypted video and audio from meetings.

With millions of people around the world working from home in order to slow the spread of the coronavirus, business is booming for Zoom, bringing more attention on the company and its privacy practices, including a policy, later updated, that seemed to give the company permission to mine messages and files shared during meetings for the purpose of ad targeting.
--
ZOOM, LE service de visioconférence dont l'utilisation a explosé au milieu de la

pandémie de Covid-19, prétend implémenter un cryptage de bout en bout, largement compris comme la forme de communication Internet la plus privée, protégeant les conversations de toutes les parties extérieures. En fait, Zoom utilise sa propre définition du terme, celle qui permet à Zoom d'accéder à la vidéo et à l'audio non chiffrés des réunions.

Avec des millions de personnes dans le monde travaillant à domicile afin de ralentir la propagation du coronavirus, les affaires sont en plein essor pour Zoom, attirant plus d'attention sur l'entreprise et ses pratiques de confidentialité, y compris une politique, mise à jour plus tard, qui semblait donner à l'entreprise l'autorisation d'exploiter des messages et des fichiers partagés lors de réunions à des fins de ciblage publicitaire.
--

REMARQUE :
La société Zoom a admis le problème sur son blog !
=> https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/
    Redirige maintenant vers => https://blog.zoom.us/a-message-to-our-users/

-> 26/03/2020
-> Zoom iOS App Sends Data to Facebook Even if You Don’t Have a Facebook Account - VICE
    => By Joseph Cox - Mar 26 2020, 2:00pm - En anglais !
    => https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account
--
Zoom's privacy policy isn't explicit about the data transfer to Facebook at all.
As people work and socialize from home, video conferencing software Zoom has exploded in popularity. What the company and its privacy policy don't make clear is that the iOS version of the Zoom app is sending some analytics data to Facebook, even if Zoom users don't have a Facebook account, according to a Motherboard analysis of the app.
--
La politique de confidentialité de Zoom n'est pas explicite sur le transfert de données vers Facebook.
Alors que les gens travaillent et socialisent à domicile, le logiciel de vidéoconférence Zoom a explosé en popularité. Ce que l'entreprise et sa politique de confidentialité ne disent pas clairement, c'est que la version iOS de l'application Zoom envoie des données d'analyse à Facebook, même si les utilisateurs de Zoom n'ont pas de compte Facebook, selon une analyse de la carte mère de l'application.
--