La sécurité de Zoom : démêler le vrai du faux

De nombreux articles de presse ont fleuri ces derniers temps, attirant l'attention sur des faiblesses réelles ou supposées de l'outil Zoom en matière de sécurité ou de données personnelles. Certaines sont à prendre en compte, beaucoup ne concernent pas notre contexte d'utilisation à l'université, et d'autres ne sont plus d'actualité.

Ce document a pour objectif de démêler le vrai du faux parmi ces différentes affirmations. Elle vous permet également, en comprenant les arguments avancés par les articles de presse et en remontant à l'information d'origine, de vous faire votre propre opinion.

Vos questions :

• Zoom a accès à mon adresse et mon numéro de carte bancaire ?

Lorsqu'un individu prend un abonnement payant à ce service, Zoom a besoin de ses informations de facturation et de paiement. C'est pourquoi leurs règles de protection des données personnelles mentionnent ces données.

Dans le cadre de l'utilisation à l'université, la licence est centralisée. Les seules informations que l'université transmet à Zoom concernant les organisateurs de réunion sont vos noms, prénoms et adresse mail, qui permettent à Zoom de s'assurer que vous êtes membre de l'université. Pour les simples participants, aucune information autre que le pseudo entré à la première connexion n'est requise de la part de Zoom.

• Zoom surveille que l'on ne s'absente pas d'une réunion ?

Zoom a développé une fonctionnalité « Suivi d'attention » qui permet à l'organisateur d'une réunion d'être prévenu quand un participant n'a plus la fenêtre Zoom en premier plan pendant plus de 30 secondes.

L'université a décidé de ne pas activer cette fonctionnalité dans son implémentation (paramétrage) de Zoom. Le 01/04, Zoom a déclaré avoir retiré cette fonctionnalité de son produit.

• Le FBI recommande de ne pas utiliser Zoom dans les écoles et la procureure de New York a porté plainte ?

Plusieurs articles ont récemment mentionné l'apparition aux États-Unis d'intrus au milieu de réunions ou de cours, diffusant des messages extrémistes ou pornographiques. Cette pratique a été appelée le « zoombombing ». Le bureau du FBI de Boston a mis en garde les écoles et la procureure de New York a demandé à Zoom de mieux lutter contre ces abus.

Le problème soulevé est lié à la diffusion publique de numéros de réunions Zoom, auxquelles n'importe qui peut se joindre. Il n'est pas lié à des faiblesses intrinsèques de l'outil.
Les bonnes pratiques consistent à ne diffuser le numéro de réunion qu'aux participants (sans les publier sur internet) et à générer un numéro de réunion spécifique pour chaque réunion sans en réutiliser un ancien. Il est également possible, et recommandé dans de nombreux usages, de protéger sa réunion par un mot de passe supplémentaire ou d'accepter les participants un par un après identification (fonctionnalité de salle d'attente).

Ces recommandations étaient présentes dans la presse informatique française ou américaine depuis plusieurs semaines et ont largement été reprises depuis (ici et ici). Depuis ces articles, les institutions apprennent de plus en plus se protéger et n'hésitent plus à prendre des mesures disciplinaires à l'égard de perturbateurs.

La DSIUN finalise la rédaction d'un guide de bonnes pratiques pour vous permettre de créer des réunions sécurisées, accessible sur https://aide-ent.pantheonsorbonne.fr.

• L'université peut accéder à l'enregistrement des réunions Zoom ?

Zoom dispose d'une fonctionnalité permettant à l'organisateur d'une réunion de l'enregistrer. L'université a décidé de ne pas activer cette fonctionnalité dans son implémentation actuelle de Zoom. De façon générale, aucune réunion Zoom ne peut aujourd'hui être enregistrée.

Dans un usage pédagogique, des amphis virtuels (avec Panopto) et des TD virtuels (avec Big Blue Button) peuvent aujourd'hui donner lieu à des enregistrements, dans un contexte contrôlé. Nous réfléchissons à un usage qui permette à un enseignant d'enregistrer au travers de Zoom une séance pédagogique dans son espace Panopto, mais cet usage n'est pas encore finalisé. La fonction d'enregistrement a également été ouverte au secrétariat des instances centrales lorsque qu'il organise ces sessions avec Zoom.

• L'organisateur d'une réunion Zoom a accès à de nombreuses données sur les participants, telles que leur localisation ?

De nombreux articles font la confusion entre l'administrateur de Zoom (celui qui possède la licence et qui paramètre l'usage de Zoom) et l'organisateur d'une réunion (hôte dans le vocabulaire Zoom).

Lorsqu'un individu prend un abonnement payant à Zoom, il est de facto administrateur et a accès aux données techniques des réunions : titre, heures de début et de fin, pseudos ou adresses mail des participants, adresses IP et localisation des participants.

Dans le cadre de l'utilisation à l'université, les organisateurs de réunions ne sont pas administrateurs, et ne peuvent accéder à ces données. Vous pouvez facilement vous en assurer en organisant une réunion, et en allant ensuite sur votre compte Zoom regarder les traces auxquelles vous avez accès.

Comme pour les autres applications, les administrateurs de Zoom sont un nombre très restreint de personnes à la DSIUN : ils ne doivent accéder aux données techniques que dans le cadre de la résolution d'incidents, et sont soumis à un devoir de confidentialité. Les réunions n'étant pas enregistrées, ils n'ont pas accès au contenu des réunions mais uniquement à leurs métadonnées.

• Zoom comprend des portes dérobées et de nombreuses failles non corrigées ?

En juillet 2019 une faille sur Apple iOS qui permettait d'accéder à la caméra sans autorisation était corrigée et rendue publique, donnant lieu à de nombreux articles et à une plainte de l'Electronic Frontier Fondation. Cette faille, signalée le 8 mars 2019 n'était cependant corrigée que le 8 juillet 2019, ce qui a été reproché à Zoom.

Deux autres failles ont été signalées le 30/03/2020 (faille MacOS et faille UNC) et corrigées le 01/04/2020. Enfin il a été rapportée que des adresses mail pouvaient être involontairement exposées (faille non corrigée à ce jour). Ces trois failles n'étaient pas exploitables dans le contexte de l'université.

Une société concurrente de Zoom lui a signalé deux failles, corrigées depuis.

Mise à jour du 15/07/2020 : Une faille concernant les systèmes sous Windows 7 ou antérieurs a été divulguée. Pour rappel, Windows 7 n'est plus maintenu par Microsoft depuis le 14/01/2020, et ne doit plus être utilisé.

Comme dans tous les logiciels informatiques (qu'il s'agisse de logiciels propriétaires ou de logiciels libres), de très nombreuses failles sont découvertes chaque jour. On ne peut que le déplorer, et Zoom n'échappe pas à la règle. Leur nombre dépend autant de la qualité intrinsèque du code du logiciel que de l'effort consenti pour découvrir ces failles. Un indicateur important à suivre est la réactivité de l'éditeur, c'est à dire le délai qu'il met pour corriger les failles qu'on lui signale.

• Zoom ne respecte pas les règles de sécurité des matériels Apple ?

Pour faciliter l'installation de son logiciel dans l'environnement iOS d'Apple, Zoom utilise des techniques similaires à celles de certains malwares, en court-circuitant les protections telles qu'un pare-feu local. Plusieurs articles ont dénoncé ce comportement (ici et ici). Il était également reproché à Zoom de ne pas supprimer l'intégralité des composants lors d'une désinstallation.
Les plus récents articles signalent que le problème a été corrigé le 02/04.

• Zoom ne chiffre pas les communications de bout en bout ?

Zoom annonce dans sa communication un chiffrage "de bout en bout". Des analyses plus poussées de la part de chercheurs ont montré que ce n'était pas le cas.

Suite à cet article, Zoom a précisé que la quasi-totalité des flux restaient chiffrés, à l'exception de ceux effectués depuis des téléphones vocaux, par opposition à un smartphone ou à un ordinateur. Il a reconnu qu'il disposait de la possibilité technique de déchiffrer une communication sur ses serveurs, et précisé qu'il n'utilisait pas cette possibilité.

L'absence d'un chiffrement "de bout en bout" est une caractéristique commune à de nombreux opérateurs (voix ou vidéos). Par exemple, un logiciel comme Jitsi (utilisé par Renater pour Rendez-vous) fonctionne de la même façon et stocke temporairement les communications sur son serveur. Le débat réside donc plus dans la confiance que l'on accorde à l'opérateur et non dans le niveau de sécurité du logiciel. Dans la pratique, l'important est que l'on chiffre les flux transitant par internet : ce sont eux qui pourraient être interceptés.

De même, le niveau de chiffrement utilisé par Zoom a également été analysé : Zoom n'utilise pas les techniques les plus avancées (ECB en 128 bits au lieu de AES en 256 bits). Le même article signale avoir remonté des failles auprès de Zoom (sans les divulguer publiquement). Zoom a récemment annoncé dans son blog que le chiffrement AES en 256 bits serait disponible prochainement.

Si votre réunion nécessite une sécurité forte, avec un chiffrage de communication de bout en bout, vous devez utiliser des services fortement sécurisés (par exemple WebConférence et Tchap, les outils sécurisés de l'Etat), qui ne font pas partie des services actuellement proposés par l'université.

• Zoom reste opaque sur les données personnelles qu'il collecte ?

Zoom a publié et a récemment mis à jour ses règles de protection des données personnelles et ses conditions de service. Elles détaillent l'ensemble des données collectées. Certains articles ont également reproché à Zoom de ne pas être assez précis sur la définition du "contenu utilisateur" ou des échanges avec ses sous-traitants, chacun pourra les consulter et se faire sa propre opinion. On peut cependant regretter qu'il n'y ait pas de différenciation plus claire entre les usages gratuits de Zoom, les détenteurs de licences individuelles (pour lesquels un numéro de carte bancaire est demandé) ou les organisateurs de réunions dans le cas d'une licence globale. De même, aucune durée de conservation n'est publiée.

Dans notre cas, les données collectées sont principalement les métadonnées des réunions : titre, heures de début et de fin, paramètres de la réunion, pseudos ou adresses mail des participants, données techniques des participants (adresses IP et localisation). Les réunions n'étant pas actuellement paramétrées pour être enregistrables, Zoom ne collecte pas le contenu des réunions (flux audio et flux vidéo).

Zoom affirme ne revendre aucune des données qu'il collecte. Contrairement à d'autres fournisseurs de services internet, le modèle d'affaires de Zoom n'est pas basé sur la publicité mais sur la vente de licences payantes à des entreprises.

Comme pour tout acteur cloud, il est cependant impossible de garantir que Zoom dit la vérité et qu'il ne fait pas un autre usage des données qu'il collecte : mais ce serait alors extrêmement risqué pour Zoom voire suicidaire, tant d'un point de vue juridique que d'un point de vue commercial.

• Zoom envoie nos données à Facebook et LinkedIn ?

L'API de connexion à Facebook, qui n'est pas utilisée dans notre contexte, échangeait des données avec Facebook sur le profil de l'utilisateur sans son consentement. Plusieurs articles s''en sont émus et Zoom assure avoir fait marche arrière. Il a cependant été reproché à Zoom de ne pas avoir été plus attentif, voire d'avoir volontairement mis en place ce mécanisme tant que personne ne s'en était offusqué.

Un mécanisme similaire avait été mis en place pour LinkedIn et Zoom s'est engagé à le retirer.

• Nos réunions peuvent être espionnées par le FBI ou la NSA ?

Zoom, société de droit américain et techniquement hébergé aux US est soumis au droit américain : des réquisitions ou des mandats peuvent lui être transmis par la justice américaine ou par des organismes étatiques. Dans ce cas-là Zoom annonce qu'il fera suite à ces demandes, comme toute société, après avoir vérifié leur validité.

Certains articles ont demandé à Zoom de communiquer les statistiques concernant ces demandes. Des sociétés comme Microsoft ou Google le font ; il apparaît que ces demandes restent rares.
Rappelons que les données concernées ne sont pas le contenu de la réunion (elles ne sont pas enregistrées) mais les métadonnées de la réunion.

Si le titre de votre réunion ou ses participants sont en lien avec la souveraineté de la France, ou si vous estimez que quoi qu'il arrive ces métadonnées ne doivent pas être communiquées, alors il est préférable que vous utilisiez des services alternatifs à Zoom tels que Rendez-vous de Renater ou BBB dans votre EPI.

• Zoom est une société d'origine chinoise ?

Zoom est une société crée en 2011. Elle a son siège à San José, en Californie. Elle est cotée au NASDAQ depuis 2019. Elle employait 1 702 personnes au 31/12/2019, dont 700 en Chine. Son fondateur et actuel PDG est M. Eric Yuan, un ancien de la société Cisco Webex.

Zoom est donc une société américaine, mais son activité commerciale en Chine et la présence d'équipes de développeurs peuvent être des moyens de pression de la part des autorités locales.

Cet article signale que des réunions Zoom ont transité par des serveurs localisés en Chine. Zoom a reconnu qu'il s'agissait d'un paramétrage fait par erreur. Zoom a annoncé qu'à partir du 18/04/2020, un paramétrage permettra de sélectionner les régions pour lesquelles les transits de données sont autorisés ou interdits. Il sera notamment possible de demander à ce que les échanges ne sortent pas en dehors de la zone Europe.

• Que se passe-t-il si je m'étais déjà abonné à Zoom à titre personnel ?

SI votre compte avait été créé avec une adresse en @univ-paris1.fr, Zoom vous proposera alors de fusionner votre ancien compte personnel avec votre nouveau compte de l'université. Vous disposerez alors de toutes les fonctionnalités souscrites par l'université.
Zoom a annoncé le 22/04/2020 une évolution de ses fonctionnalités de fusion d'un compte personnel, non encore testées par la DSIUN.

Attention, si votre interlocuteur organise une réunion depuis un compte personnel en dehors des adresses @univ-paris1.fr, l'université n'en a pas la maîtrise : votre interlocuteur aura alors la possibilité d'enregistrer une réunion ou d'utiliser les fonctions administrateur de son compte.

• Des comptes Zoom sont en vente sur le dark web ?

Des articles de presse mentionnent que 530 000 comptes Zoom (identifiant/mot de passe) sont en vente sur des forums clandestins sur internet. Il s'agirait de couples identifiants / mort de passe en provenance de piratage d'autres sites. De nombreux utilisateurs ayant la mauvaise pratique de réutiliser le même mot de passe pour tous leurs usages, des pirates ont "testé" sur Zoom ces mots de passe volés et les mettent en vente.
Ce n'est donc pas la qualité du code de l'application Zoom qui est mis en cause (toute autre application peut être victime de la même manipulation), mais le simple fait qu'elle soit populaire, ce qui rend ce type de malversations attractif pour des pirates.

• Des failles zéro day sont en vente sur le dark web ?

Cet article de presse mentionne que deux failles zéro day sont en vente sur des forums clandestins sur internet. Une faille zéro day est une faille qui a été découverte mais pas encore divulguée ni corrigée : celui qui en a connaissance peut ainsi l'exploiter en exclusivité.
L'article mentionne que pour exploiter la faille il faut déjà être connecté à la réunion, ce qui en réduit l'intérêt. Il faudra cependant surveiller attentivement si Zoom détecte qu'elle est exploitée et la corrige.

• Parmi tous ces problèmes évoqués, lesquels sont toujours d'actualité ?

- Zoom reste une société étrangère, qui héberge ses données à l'étranger : elle est soumise aux réquisitions judiciaires américaines (Cloud Act) et peut avoir des pressions de la part de la Chine. Pour toute réunion liée à la souveraineté nationale, il faut utiliser une autre solution

- Zoom est une solution populaire, très répandue : de nombreux pirates recherchent sur internet des codes de réunions non protégées disponibles, des enregistrements de réunions, des mots de passe, ... Il est très difficile pour Zoom de s'en protéger, la sécurité repose sur les bonnes pratiques des utilisateurs
- La communication de Zoom sur ses règles de protection des données personnelles est incomplète
- Depuis le 01/06/2020, les comptes payants de Zoom (c'est le cas de l'université) bénéficient du chiffrement de bout en bout, et chacun a du mettre à jour son logiciel Zoom pour en bénéficier. Les utilisateurs qui se connectent à une réunion à l'aide d'un téléphone vocal ne bénéficient pas de ce chiffrement.
- La procédure d'installation sur Mac ne respecte pas les règles de sécurité fixées par Apple
- Une faille concernant la fonction "salle d'attente" a été communiquée à Zoom par un chercheur en sécurité. On ne connaît pas sa gravité. Il faudra surveiller si Zoom propose une correction prochainement
- Deux failles zéro day seraient en vente, Il faudra surveiller si Zoom détecte qu'elle est exploitée et la corrige

Zoom fait actuellement évoluer très régulièrement son produit et diffuse de nouvelles mises à jour : certaines des informations ci-dessus sont peut-être déjà obsolètes.

Si vous souhaitez consulter d'autres articles analysant la sécurité de Zoom :

Zoom publie un blog en français, comportant de nombreuses réponses concernant la sécurité.
Une page très complète de conseils a été rédigée par la fondation Mozilla.
Récemment, Orange Cyberdéfense a réalisé une analyse très complète de la sécurité de Zoom (en anglais).

Pour des articles indépendants de Zoom :
https://www.lemondeinformatique.fr/actualites/lire-zoom-en-eaux-troubles-sur-la-securite-et-la-confidentialite-78653.htm
https://www.lemondeinformatique.fr/actualites/lire-zoom-sur-les-ameliorations-securite-de-zoom-78725.html
https://www.silicon.fr/securite-vie-privee-zoom-337383.html
https://www.silicon.fr/zoom-course-contre-montre-337809.html
https://www.schneier.com/blog/archives/2020/04/security_and_pr_1.html
https://www.tomsguide.com/news/zoom-security-privacy-woes
https://medium.com/@0xamit/zoom-isnt-malware-ae01618e2046
https://medium.com/@vince_17729/zooming-to-conclusions-20560d9f40b9
https://www.linkedin.com/pulse/strange-zoom-pile-on-robert-walker/?trackingId=fVWI6CZXRE6H9xLRIHniPg%3D%3D
https://business.financialpost.com/pmn/business-pmn/video-service-zoom-taking-security-seriously-u-s-government-memo

Vous trouverez également dans ces articles, ou plus généralement dans la presse, des communiqués d'institutions qui interdisent ou déconseillent l'usage de Zoom : certains de ces avis sont accompagnés d'arguments et sont intéressants à étudier, mais beaucoup mentionnent une décision sans en expliquer les raisons. Il semble qu'un certain emballement ou un principe de précaution excessif ait conduit des organismes à interdire l'usage de Zoom sans même étudier ce qui pouvait lui être reproché.

En conclusion

Dès le début du confinement, les outils de visioconférence historiquement préconisés par l'université (**RENAvisio et Rendez-vous de Renater**) ont rencontré des problèmes de disponibilité. De nombreux enseignants ou personnels administratifs ont cherché à assurer une continuité avec différents outils, gratuits ou payants : Skype, Teams, Zoom, Hangout, Discord, Snapchat, ...

Une solution à l'échelle de l'université, basée sur Zoom et sécurisée par la DSIUN, nous a paru être une solution acceptable même si elle n'est pas parfaite.

Rappelons que, pour des réunions qui nécessiteraient un haut niveau de confidentialité ou pour des utilisateurs qui n'auraient pas confiance dans Zoom, **la solution Rendez-vous de Renater** reste accessible et est totalement supportée par la DSIUN. De même, l'utilisation pour les usages pédagogiques de la solution d'**amphis virtuels (Panopto)** ou de **TD virtuels (BBB)** vous garantit que les données ne sortent pas du cadre de l'université.

Une grande partie de la sécurité de vos réunions résidera maintenant dans une bonne prise en main et une maîtrise des possibilités de l'outil par chacun.

Note : Si des affirmations contenues dans ce mémo vous paraissent erronées, ou si vous avez entendu parler d'un problème de sécurité qui ne figure pas ici et qui mériterait d'être mentionné, vous pouvez écrire à : rssi@univ-paris1.fr