Zoom sur la sécurité de Zoom !

Suite à son incroyable succès lié à la crise sanitaire, Zoom a fait l'objet d'une attention particulière des chercheurs en sécurité et leurs découvertes ont entrainé une avalanche de critiques. Alors qu'en est-il véritablement ? Peut-on raisonnablement utiliser Zoom dans un contexte professionnel ? C'est ce que nous allons voir dans cet article.

- Préambule
- Fuite de données personnelles vers Facebook
- Problème du « Zoom Bombing »
- Zoom et le chiffrement de bout en bout
- Fuite de mots de passe et exécution de code via UNC

- Problèmes de sécurité dans OSX (Mac)
- Damned, nos données transitent par la Chine !
- Pour conclure

Préambule

Zoom est une solution de visioconférence basée sur un service Cloud en mode SaaS associé à un logiciel client disponible pour PC, Mac, Android et iOS. Avec la crise sanitaire du COVID-19 et la généralisation des réunions à distance, Zoom a vu son nombre d'utilisateurs passer de 10 millions à plus de 200 millions en quelques semaines. Derrière le produit, il y a la société Zoom Video Communications, société américaine basée à San Jose (Californie). En seulement un trimestre et alors que tous les marchés financiers se sont écroulés, sa capitalisation boursière au NASDAQ a plus que doublé avec une action valorisée à 146 $ au 31 mars 2020 (68 $ au 1er janvier). Alors bien évidemment, devant un tel succès et avec toutes les inquiétudes liées à la sécurité du télétravail, bon nombre de chercheurs en sécurité se sont lancés dans la recherche de vulnérabilités dans le produit star du moment.

Zoom est une solution technologique complexe et dans tout logiciel complexe, quand on cherche activement des failles et bien vous savez quoi ? On en trouve ! Et ce n'est certainement pas Microsoft, Google ou Apple qui vous diront le contraire. Il ne faut donc pas juger la sécurité d'une solution Cloud uniquement sur le nombre et la criticité de ses vulnérabilités car il faut également prendre en compte la capacité du fournisseur à réagir et à répondre rapidement et correctement aux problèmes de sécurité rencontrés. Mais soyons factuel et regardons les problèmes identifiés ces dernières semaines.

Fuite de données personnelles vers Facebook

Tout est parti d'un article de Joseph Cox qui dévoile le 26 mars 2020 que

l’application Zoom envoie les données personnelles des utilisateurs à Facebook et ceci même si l’on ne dispose pas de compte Facebook.

Le problème était lié à une mauvaise utilisation du SDK Facebook sur les plateformes iOS et ne concernait donc que les clients Zoom sur iPhone et iPad. Les données personnelles divulguées étaient en fait des diagnostics de base des iPhone ou iPad (taille de l’écran, espace de stockage, …). Et contrairement à ce que j’ai pu lire un peu partout sur le Net et notamment dans les réseaux sociaux, il n’y avait aucune information sensible comme un nom d’utilisateur, un mot de passe, un numéro de téléphone ou encore le contenu des conversations.

Selon des informations disponibles sur son Blog, Zoom a découvert le problème le 25 mars et a publié un client Zoom corrigé pour iOS dès le 27 mars 2020. Deux jours pour corriger un bug de sécurité, j’aimerais bien que ce soit la règle chez tous les éditeurs. En tout cas, on ne peut pas reprocher à Zoom de ne pas avoir rapidement réagi sur ce problème qui est aujourd’hui définitivement réglé.

Problème du « Zoom Bombing »

Dans Zoom, il est possible d’accéder directement à une réunion privée (si le créateur de la session l’a autorisé) via un simple code (ID meeting) composé de 9 à 11 chiffres. Et bien entendu, il est possible avec un « bot » de trouver des codes de conférence valides et de s’introduire dans la conférence. On a également vu plusieurs cas où le code de conférence était publié ou divulgué et de nombreux intrus venaient perturber les conférences.

Pour la réponse aux attaques par un Bot, il s’agit ici d’un problème de conception et Zoom devra changer l’entropie de ses codes de conférence par quelque chose de beaucoup plus robuste. Un mécanisme anti brute force sur le service SaaS associé à un ID de conférence codé sur 12 caractères (alpha & num) devrait faire l’affaire.

Mais sans attendre ces évolutions en matière de sécurité, on peut d'ores et déjà résoudre le problème du Zoom bombing par la mise en place d'un contrôle en amont. On peut en effet dans Zoom protéger l'accès à une conférence par exemple via une liste d'adresses e-mail autorisées. D'autre part, Zoom a ajouté récemment une fonctionnalité de salle d'attente. Ainsi les retardataires sont placés en liste d'attente afin de valider leur participation à la réunion. Zoom a également ajouté la possibilité de saisir un mot de passe pour entrer en conférence.

Zoom et le chiffrement de bout en bout

Ici tout est parti d'un article de Micah Lee et Yael Grauer le 31 mars qui dévoilait que, contrairement aux affirmations de Zoom, les réunions n'étaient pas chiffrées de bout en bout. Et effectivement, le chiffrement des conférences Zoom n'est pas un « vrai » chiffrement de bout en bout que l'on appelle E2E (End-to-End Encryption). Les conférences sont effectivement protégées par un chiffrement et pour cela Zoom utilise le protocole SRTP (Secure Real-time Transport Protocol) avec un chiffrement AES-128. Mais les clés de 128 bits utilisées sont générées par les serveurs Zoom et distribuées via TLS aux clients Zoom. Par conséquent, Zoom peut avoir accès à l'intégralité des données échangées entre les participants. Dans une véritable communication E2E, seuls les participants de la communication ont accès aux clés de chiffrement mais pas les intermédiaires qui relaient les communications. C'est par exemple le cas avec l'application Signal ou avec Face Time d'Apple. Mais dans les deux cas, ces solutions ne permettent pas une montée à l'échelle, c'est-à-dire une communication avec des centaines de participants.

D'autre part, des chercheurs du laboratoire Citizen Lab de l'université de Toronto ont publié le 3 avril un article sur les algorithmes cryptographiques utilisés par Zoom. Comme indiqué précédemment, la communication des vidéos est bien chiffrée en AES-128 mais Zoom utilise AES en mode ECB. Or ce mode de chiffrement a des faiblesses connues et le standard SRTP recommande d'utiliser AES avec d'autres modes comme CTR ou f8. En ce sens, on peut dire que Zoom n'est clairement pas à l'état de l'art en matière de cryptographie.

On pourrait synthétiser ce problème de chiffrement E2E sous forme de questions / réponses :

- La solution actuelle de Zoom est-elle à l'état de l'art en matière de communication sécurisée ?
  - Non

- Peut-il y avoir violation de la confidentialité des échanges ?
  - Oui selon 3 scénarii possibles : malveillance interne chez Zoom, faille de sécurité critique dans le service Zoom ou requête gouvernementale (mandat FISA, NSL Freedom act ou assignation CLOUD act.)

- Peut-on techniquement réaliser une véritable solution multi-utilisateurs en E2E ?
  - Oui, mais c'est relativement difficile à faire.

- Est-ce une fonctionnalité qui sera prochainement disponible dans Zoom ?
  - Peut-être à terme mais sans doute pas avant la disponibilité du vaccin contre le COVID-19…

Fuite de mots de passe et exécution de code via UNC

Ici tout commence le 31 mars 2020 avec un article de Lawrence Abrams. Dans Zoom les participants à une réunion peuvent communiquer entre eux en s'envoyant des messages texte via une interface de discussion. Et si un message échangé contient une URL alors celle-ci est automatiquement convertie en hyperlien afin que les autres

membres puissent accéder à l'information via un simple clic. Le problème est qu'un chercheur en sécurité a découvert que le client Zoom convertissait également les chemins UNC en un lien cliquable dans les messages de discussion. Ainsi, si un utilisateur clique sur un lien de chemin UNC, Windows tentera de se connecter au site distant en utilisant le protocole de partage de fichiers SMB et ce faisant, Windows enverra par défaut le nom de connexion de l'utilisateur et le hash de son mot de passe NTLM. Et bien évidemment, si le mot de passe n'est pas robuste, un outil comme hascat associé à une puissante carte graphique pourra permettre de découvrir le mot de passe de l'utilisateur. Et puis au-delà de la fuite de l'identifiant et du hash du mot de passe, on découvre également un autre problème. En effet, en utilisant une UNC sur le localhost (127.0.0.1), on peut lancer l'exécution d'un programme sur l'ordinateur d'un participant.

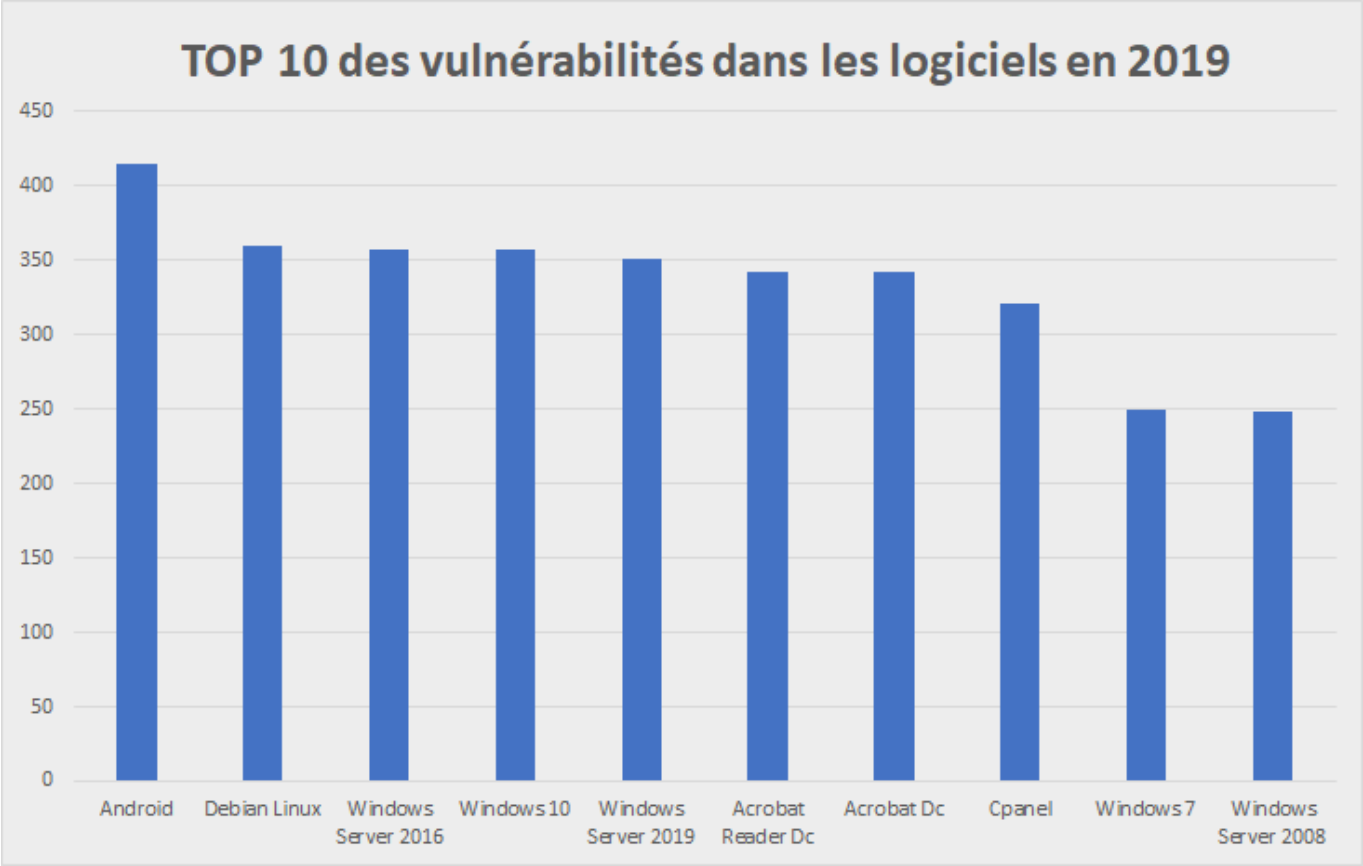
En réponse à ces problèmes, Zoom a publié dès le 1er avril, la version 4.6.19253.0401 de son client qui empêche désormais tous les liens publiés, y compris les URL normales et les chemins UNC, d'être convertis en hyperliens cliquables. Alors là aussi, on pourrait demander de manière irréaliste à Zoom de délivrer un logiciel sans faille. Mais que demander de plus lorsqu'un problème de sécurité est identifié le 31 mars et que la solution est disponible dès le lendemain. Je le répète, j'aimerai bien que tous les éditeurs soient aussi réactifs et professionnels face à ces problématiques de sécurité.

Problèmes de sécurité dans OSX (Mac)

Le 30 mars, un chercheur en sécurité a découvert que Zoom utilisait une technique pas très « catholique » pour installer son application cliente pour Mac. L'idée pour Zoom était de permettre une installation facile sans avoir le consentement de l'utilisateur final. Mais comme cette technique est généralement utilisée par les cybercriminels dans l'écriture de malwares pour OSX, la news publiée sur twitter a rapidement fait le buzz (8000 likes en moins d'une semaine pour un chercheur quasiment inconnu sur twitter le 29 mars).

Là aussi, Zoom a rapidement réagi et a proposé dès le 2 avril un client MacOS exempt

des « hacks » d'installation incriminés. Dans cette version pour OSX, Zoom a également corrigé deux autres vulnérabilités importantes. Une permettait une élévation de privilège et l'autre permettait à un code malveillant d'accéder au micro et à la caméra du Mac à l'insu de l'utilisateur. Des failles critiques, je vous l'accorde, mais voulez-vous que l'on parle du nombre de failles critiques découvertes chaque année dans Windows ? Et allez-vous pour autant passer sous Linux ? Tiens juste pour info, regardons le palmarès des vulnérabilités découvertes en 2019 (source : www.cvedetails.com) :



Damned, nos vidéos transitent par la Chine !

En fonctionnement normal, le client Zoom essaie de se connecter à un datacenter principal défini dans une liste de datacenters situés dans sa région géographique ou à proximité. Si ces multiples tentatives de connexion échouent en raison d'une congestion réseau ou d'un autre problème, le client essaie alors de se connecter à un datacenter secondaire défini dans une liste de secours. Mais en février, en raison de la crise COVID, Zoom a dû augmenter très rapidement sa capacité sur la

région chinoise pour faire face à une augmentation massive de la demande. Et dans la précipitation, ils ont ajouté par erreur leurs deux datacenters chinois à des listes de secours. Cela signifie que certains clients non chinois ont pu voir leurs communications transiter par la Chine.

Zoom par la voix de son CEO Eric S. YUAN a indiqué avoir supprimé immédiatement ses deux centres de données chinois des listes de secours dès qu'ils ont eu connaissance du problème. Et cela explique certainement pourquoi les chercheurs de Citizen Lab ont vu des clés de chiffrement distribuées par des serveurs chinois à des clients Zoom situés hors de Chine.

Pour conclure

Alors après toutes ces révélations, est-il encore raisonnable d'utiliser Zoom ?

S'il s'agit d'organiser des conférences ou des réunions d'entreprise dans lesquelles aucune information particulièrement sensible n'est communiquée, la réponse est bien évidemment oui. Zoom est une solution performante, facile à utiliser et même gratuite jusqu'à 100 participants. C'est la raison de son succès et sur ce point, il n'y a tout simplement pas de concurrence. Par exemple, je vais prochainement animer en distanciel deux séminaires pour Orsys : Sécurité du Cloud (28-29 avril) et Cybersécurité (4-6 mai). Les sessions s'effectueront avec Zoom et pour cela, c'est vraiment l'application idéale.

Mais on a appris ces derniers jours que Zoom était également utilisé par les dirigeants de plusieurs pays (avec entre autres Emmanuel Macron, Boris Johnson et Vladimir Poutine). Alors peut-on utiliser Zoom pour des réunions gouvernementales ? La réponse est évidente, c'est clairement non. Sans tomber dans la paranoïa, on imagine bien l'attractivité que peut représenter une telle plateforme pour des services de renseignement gouvernementaux. D'autant qu'il n'est pas toujours utile

de travailler à la NSA pour accéder à ce type de réunion puisque que parfois c'est le 1er ministre (Boris Johnson) qui publie lui-même (certes accidentellement) l'identifiant secret de la réunion gouvernementale sur Twitter.

Alors en guise de conclusion, on peut dire qu'utilisée à bon escient et avec la prudence qui s'impose, Zoom est une solution adaptée aux circonstances exceptionnelles liées à la crise sanitaire. Pour des réunions sensibles, il faudra sans doute se tourner vers des solutions (théoriquement) plus sûres et (certainement) plus chères. On peut par exemple citer la solution de visioconférence de la société Montpellieraine Tixeo qui est certifiée (CSPN) et qualifiée (niveau élémentaire) par l'ANSSI.