Sécurité et vie privée : Zoom est-il à la hauteur ?

Faut-il vraiment utiliser Zoom ?

La popularité de ce logiciel de communication est montée en flèche avec la pandémie de coronavirus Covid-19.

L'attention portée aux enjeux de sécurité et de vie privée a crû en parallèle.

En la matière, il y a des choses à redire. Notamment au sujet du chiffrement de bout en bout. Celui-ci n'est effectif ni pour l'audio, ni pour la vidéo, contrairement à ce que laisse entendre la présentation du produit. Les données en question ne sont en l'occurrence protégées que lors de leur transport.

Zoom se réserve en outre le droit de collecter et de partager du « contenu utilisateur » – terme qui englobe de nombreuses données. Face aux inquiétudes, l'éditeur a récemment apporté une clarification à propos de ses pratiques. Il a, entre autres, exclu toute exploitation d'informations à des fins publicitaires.

Contacts inconnus

Toujours au chapitre vie privée, des utilisateurs (qui se compteraient au moins par milliers) ont vu une foule d'inconnus apparaître dans leur liste de contacts.

Le problème semble lié à une fonctionnalité qui met automatiquement en relation les comptes associés à des adresses e-mail dépendant d'un même domaine, et donc censés travailler pour une même organisation. Les principaux fournisseurs de messagerie (Gmail, Hotmail, Yahoo…) sont naturellement exclus du dispositif. Mais les plus petits fournisseurs ne le sont pas…

> *@zoom_us I just had a look at the free for private use version of Zoom and registered with my private email. I now got 1000 names, email addresses and even pictures of people in the company Directory. Is this intentional? #GDPR pic.twitter.com/bw5xZIGtSE*
>
> *— Jeroen J.V Lebon (@JJVLebon) March 23, 2020*

Windows : attention à la fuite d'identifiants

Autre élément à avoir attiré l'attention : l'application Zoom pour iOS. Le SDK Facebook intégré avait tendance à envoyer un grand nombre de données au réseau social, que l'utilisateur en soit ou non membre.

L'éditeur a corrigé le tir la semaine passée.
Il n'a, en revanche, pas encore éliminé la faille découverte dans son client Windows.

Celui-ci traduit en liens cliquables les URL de type UNC (Universal Naming Convention), qui pointent vers des ressources réseau.

Lorsque l'utilisateur clique sur ce type de lien, le protocole d'authentification NTLM (NT Lan Manager) s'enclenche. Par défaut, il transmet l'identifiant Windows… et le hash du mot de passe, qui peut être craqué en quelques secondes avec des outils accessibles gratuitement.

> *#Zoom chat allows you to post links such as \\x.x.x.x\xyz to attempt to capture Net-NTLM hashes if clicked by other users.*
>
> *— Mitch (@_g0dmode) March 23, 2020*

> *Hi @zoom_us & @NCSC – here is an example of exploiting the Zoom Windows client using UNC path injection to expose credentials for use in SMBRelay attacks. The screen shot below shows an example UNC path link and the credentials being exposed (redacted). pic.twitter.com/gjWXas7TMO*
>
> *— Hacker Fantastic (@hackerfantastic) March 31, 2020*

Ces mêmes liens permettent aussi de lancer des programmes en local. Y compris sans que l'utilisateur soit averti.

> *That's just MoTW, I've verified it works. No prompts required. I think someone could realistically click on that. pic.twitter.com/VwYGB5il48*
>
> *— Tavis Ormandy (@taviso) April 2, 2020*

Sur Mac aussi

La version Mac de Zoom n'est pas épargnée. Elle abrite des vulnérabilités qui ouvrent la voie à :

- Une élévation de privilèges
  L'action est rendue possible par le fonctionnement de l'installeur de Zoom. Celui-ci est conçu de sorte à pouvoir installer l'application avec une intervention minimale de la part de l'utilisateur. Voire sans intervention du tout. Il obtient pour cela un accès root, éventuellement à travers l'API AuthorizationExecuteWithPrivileges, qu'Apple considère pourtant comme obsolète. Un tiers peut obtenir cet accès root en modifiant ou en remplaçant un script que déploie l'installeur.

> *Ever wondered how the @zoom_us macOS installer does it's job without you ever clicking install? Turns out they (ab)use preinstallation scripts, manually unpack the app using a bundled 7zip and install it to /Applications if the current user is in the admin group (no root needed). pic.twitter.com/qgQ1XdU11M*
>
> *— Felix (@c1truz_) March 30, 2020*

- L'espionnage du micro et de la webcam
  Et plus globalement l'usage des mêmes permissions que celles dont dispose l'application,

par injection de code dans le processus.

On portera également attention au phénomène dit du « zoombombing ». C'est-à-dire les accès indésirables à des réunions. La pratique s'est développée avec le contexte actuel. Pour se l'épargner, il est recommandé, d'une part, de protéger chaque réunion par un mot de passe. Et de l'autre, d'utiliser les salles d'attente, où les utilisateurs patientent avant qu'un administrateur les autorise à rejoindre la discussion.

Photo d'illustration © Zoom