G Suite : vers un « Cambridge Analytica des entreprises » ?

Vers un scandale « à la Cambridge Analytica » chez Google ? Michael Lack et Irwin Reyes ne l'affirment pas. Mais ils soulèvent la question dans une étude présentée au 41e Congrès de l'IEEE sur la sécurité et la vie privée.

Les deux chercheurs, qui travaillent pour l'entreprise américaine Two Six Labs, se sont intéressés à la *marketplace* G Suite. En date du 2 janvier 2020, le catalogue comptait 1 392 applications web censées être utilisables avec la suite bureautique.

Lack et Reyes ont pu en connecter 987 d'entre elles à un compte Google (@gmail.com). La plupart de celles qu'ils ne sont pas parvenus à connecter requéraient un compte administrateur G Suite.

La majeure partie de ces 987 applications demandaient au moins une autorisation d'accès *via* l'API Google (889 en l'occurrence).

Authorization	% apps
Display and run third-party web content in prompts— and sidebars inside Google applications.	50%
Connect to an external service.	49%
See, edit, create, and delete your spreadsheets in Google Drive.	27%
Allow this application to run when you are not present.	25%
See, edit, create, and delete all of your Google Drive files.	21%
View and manage your Google Docs documents.	13%
Run as a Gmail add-on.	11%
View and manage data associated with the application.	11%
Send email as you.	10%
View users on your domain.	9.0%

TABLE I
10 MOST COMMON AUTHORIZATIONS, N = 987 APPS

Mystérieux services

La permission le plus fréquemment demandée (50 % des cas) consiste à afficher et exécuter du contenu web au sein des applications de la suite bureautique.

Vient ensuite la permission de contacter un service externe (481 applications). Et sur ce volet, c'est le flou. On ne peut compter que sur les développeurs pour préciser la nature desdits services dans

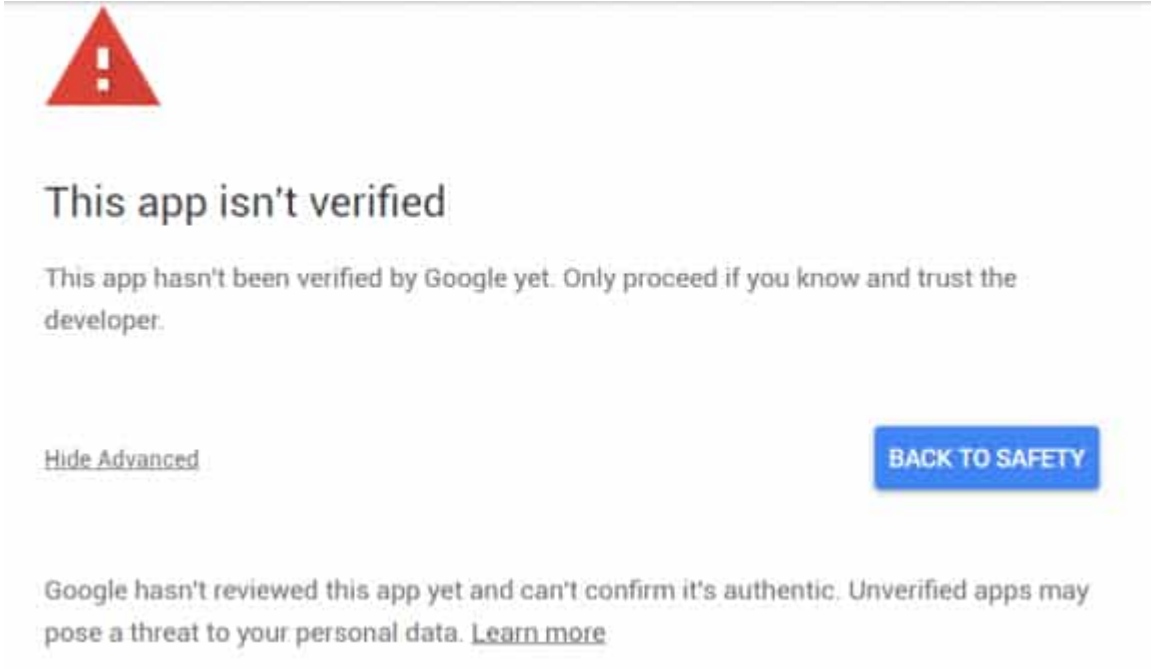
la description de leurs applications. Mais c'est loin d'être systématique, affirment les chercheurs.

En combinant les permissions, on obtient, parmi ces 481 applications :

- 103 autorisées à manipuler des fichiers Google Drive (lecture, écriture, suppression)
- 81 autorisées à lire les messages Gmail
- 15 autorisées à manipuler le répertoire de contacts Google

Il existe une procédure de contrôle préalable à la publication des applications sur la *marketplace*.
Elle peut durer plusieurs jours pour les utilisations « sensibles » de l'API.Et plusieurs semaines pour les utilisations que Google qualifie de « restreintes ».

Compte tenu de ces délais, Google autorise la publication avant approbation. Les applications qui sont dans ce cas affichent un message d'alerte avant la connexion à un compte Google. Elles sont par ailleurs soumises à une limite de 100 installations, avec des ajustements possibles « sur la base de l'historique de l'application, de la réputation du développeur et du risque ».



Sur l'ensemble des applications examinées le 2 janvier, 277 applications étaient dans ce cas.
Lack et Reyes ont pu en connecter 144 à leur compte. Parmi elles, les demandes d'autorisation d'accès à l'agenda et aux contacts sont plus fréquentes que sur l'ensemble de l'échantillon des 987.

Le modèle Android

Deux semaines plus tard (le 18 janvier 2020), l'essentiel de ces 144 applications (124) avaient toujours le statut « non vérifié ».
24 avaient par ailleurs dépassé les 100 connexions de comptes Google, avec les mêmes autorisations que le 2 janvier – ce qui semble exclure un éventuel passage au statut « vérifié », puis un retour au « non vérifié ».

Une application en particulier a enregistré plus de 1 000 connexions de comptes dans cet intervalle de 2 semaines : ezShared Contacts. Elle requiert la connexion à un service externe, mais aussi un plein accès à Gmail en lecture/écriture.

Lack et Reyes émettent plusieurs recommandations :

- Demander les autorisations nécessaires non lors de la connexion de l'application au compte Google, mais à l'exécution, comme c'est le cas sur Android.
  C'est, selon les chercheurs, d'autant plus important que Google n'explique pas précisément quelles fonctions API sont « sensibles ». Tout au plus s'agit-il, dans sa nomenclature, de celles qui « permettent l'accès à des données d'un utilisateur ».
- Profiter du fait que certains développeurs implémentent et déploient leurs applications avec Google Apps Script.
  Les applications qui sont dans ce cas fonctionnent sur l'infrastructure cloud de Google. Lequel pourrait donc fournir des informations sur les services externes contactés.
- Appliquer, à l'image de Facebook après l'affaire Cambridge Analytica, des restrictions API.
  Le réseau social a limité la quantité de données communicables par ce biais et a imposé une révocation de l'accès après 90 jours sans interaction.
  Google ne semble pas disposer de ce mécanisme, notent Lack et Reyes.

Illustration principale © Google