Slack : un canal de phishing dans les espaces de travail

Utilisateurs de GitHub, attention à ce que vous mettez dans vos dépôts publics.
La dernière publication des Alien Labs d'AT&T le rappelle. Le sujet : une vulnérabilité dans Slack.

À la racine, les *webhooks* entrants.
Cette fonctionnalité permet d'exposer les espaces de travail à des applications tierces afin qu'elles puissent leur transmettre des données (en HTTP, au format JSON).

Le système est considéré comme peu risqué pour plusieurs raisons :

- Les *webhooks* entrants, comme leur nom l'indique, ne permettent que la réception de données.
- Les URL uniques sur lesquels ils reposent (modèle ci-dessous) sont secrètes.
- Il faut obligatoirement spécifier un canal cible, ce qui réduit en théorie la surface d'attaque.

```
https://hooks.slack.com/services/T00000000/B00000000/XXXXXXXXXXXXXXXXXXXXXXXX
```

Cela dit, ont constaté les chercheurs d'AT&T :

- Il existe une option qui permet de remplacer le canal cible par un autre… et éventuellement d'y modifier les droits de publication.
- Une recherche sur les dépôts GitHub publics a suffi à obtenir plus de 130 000 résultats contenant des URL de *webhooks*.

D'après la documentation de Slack, l'étendue des canaux cibles autorisés dépend du créateur du *webhook*. Le risque est donc maximal lorsqu'il s'agit d'un administrateur.

Du *phishing*… éventuellement

L'exploitation combinée de ces paramètres ouvre la porte à des exfiltrations de données. Dans les grandes lignes, on :

- Crée une application installable par tout le monde.
- Envoie des messages aux URL dont on dispose pour faire en sorte qu'un utilisateur (ou un *bot*) installe l'application.
- Récupère la clé d'accès dudit utilisateur pour bénéficier des autorisations qui lui sont données sur l'espace de travail.

La sécurité étant basée sur le contexte, certains profils sont plus « lucratifs ». Ils offrent d'autant plus de possibilités, dont l'envoi de messages privés à d'autres utilisateurs. Et la propagation entre espaces de travail en exploitant les canaux partagés.

Comment se prémunir ?

Par défaut, tous les membres d'un espace de travail peuvent y installer une application. C'est au propriétaire d'activer les différents systèmes d'approbation disponibles. Entre autres :

– Se limiter au catalogue d'applications validées par Slack
– Approuver les applications manuellement ou sur la base d'une liste blanche
– Utiliser les *logs* pour détecter les authentifications OAuth suspectes

Du côté de Slack, on pourrait implémenter le principe du « moindre privilège » pour les webhooks. Notamment en n'autorisant pas par défaut la modification du canal cible.

Officiellement, l'entreprise américaine a pour l'instant choisi de détecter les URL exposées au public sur GitHub… et de les invalider.

Illustration principale © Slack