Messagerie instantanée : l'aperçu des liens, fonctionnalité à risques ?

Les aperçus de liens, point faible des messageries instantanées ? On est tenté de l'affirmer à la lumière d'une étude qu'ont menée deux développeurs.

Le tableau ci-dessous liste les services qu'ils ont testés.

App Name	iOS Version	Android Version
Discord	39.0	38.4
Facebook Messenger	280.0.0.32.106	8.61.0
Google Hangouts	35.0.324846370	35.0.327050771
Instagram	v158.1.0.29.120	158.0.0.30.123
LINE	10.14.0	10.15.2
LinkedIn	9.16.387	4.1.489
Reddit	2020.34.0.307260	2020.33.1.28759202
Slack	20.09.10	20.09.10.0
Twitter	8.37.1	8.63.0-release.00
Viber	13.8.0	13.8.1.0
Zoom	5.2.2 (45104.0831)	5.2.2 (45092.0831)
[redacted]	[redacted]	[redacted]

Les expérimentations se sont limitées à la partie chat. Mais elles suffisent à faire ressortir un large panorama d'usages… et de risques.

Trois méthodes se dégagent pour générer les aperçus des liens :

- Le faire côté expéditeur
  C'est ce qui se passe sur iMessage, Viber et WhatsApp. Ainsi que sur Signal, si l'option de prévisualisation des liens est activée.

- Le faire côté destinataire
  Deux applications étaient dans ce cas au moment des tests. D'une part, Reddit. De l'autre, l'app « mystère », masquée dans le tableau ci-dessus, officiellement le temps de corriger les problèmes que lui ont signalés les chercheurs.
- Le faire sur un serveur tiers
  Discord, Hangouts, Instagram, LINE, LinkedIn, Messenger, Slack, Twitter et Zoom emploient cette méthode.

Méthode « serveur » : que deviennent les données ?

Les deux premières solutions peuvent poser des problèmes de consommation de ressources. Avec, en l'occurrence, des applications qui téléchargent un contenu dans son intégralité pour en générer un aperçu. Reddit était dans ce cas ; Viber l'est encore.

Le même problème s'est présenté avec plusieurs applications qui génèrent les aperçus côté serveur. Notamment Instagram et Messenger. Un fichier de 2,6 Go a engendré un total de 24,7 Go de données émises, vers non pas un, mais plusieurs serveurs.

La « méthode serveur » pose un autre problème, du domaine de la *privacy* : que deviennent les données transmises ? Rares sont les fournisseurs qui communiquent des informations à ce sujet. Slack se distingue en annonçant une durée de conservation de 30 minutes environ. Pour les autres, on sait essentiellement le volume maximal de données que le serveur récupère :

- 15 Mo pour Discord
- 20 Mo pour Hangouts et LINE
- 25 Mo pour Twitter
- 30 Mo pour Zoom
- 50 Mo pour LinkedIn et Slack
- Sur Instagram et Messenger, tout le fichier s'il s'agit d'une image ou d'une vidéo

Adresses IP et JavaScript

Les chercheurs s'attardent sur le cas de LINE, qui utilise la « méthode serveur » alors même que sa messagerie est censée être chiffrée de bout en bout.

Ils déplorent aussi le fait que certains serveurs (Instagram et LinkedIn) aient exécuté le code JavaScript vers lequel pointait un lien de test. Au risque que ledit code soit malveillant.

Autre remarque, concernant cette fois les méthodes « expéditeur » et « destinataire » : pour générer l'aperçu d'un lien, l'application transmet au serveur qui héberge le contenu l'adresse IP de l'utilisateur. Ce qui peut trahir approximativement sa géolocalisation.

Illustration principale via *visualhunt.com*