Android aux prises avec une menace qui veut voler notre argent

Vincent Paquette ⁝

Capture d'écran, pour visionner la vidéo, cliquer le lien suivant de François Charron:

Android aux prises avec une menace qui veut voler notre argent (francoischarron.com)

Des chercheurs en sécurité informatique de chez ThreatFabric ont identifié une nouvelle menace qui rôde dans l'univers Android.
Il s'agit du logiciel malveillant Brokewell.
Ce dernier se dissimule dans de fausses mises à jour de sécurité.
Il a pour but d'accéder à nos applications bancaires et voler notre argent.

L'univers Android doit faire face à une menace importante avec Brokewell. - *francoischarron.com avec Dall-E*

On le sait, si on possède un téléphone Android, on a tout intérêt à mettre un bon antivirus dedans.

Bien que l'univers Android offre plus de possibilités avec son système ouvert, il reste que ceci ouvre justement la porte à davantage de menaces.

L'une d'entre elles est en train d'émerger et a pour nom: Brokewell.

Un virus dans de fausses mises à jour de Chrome

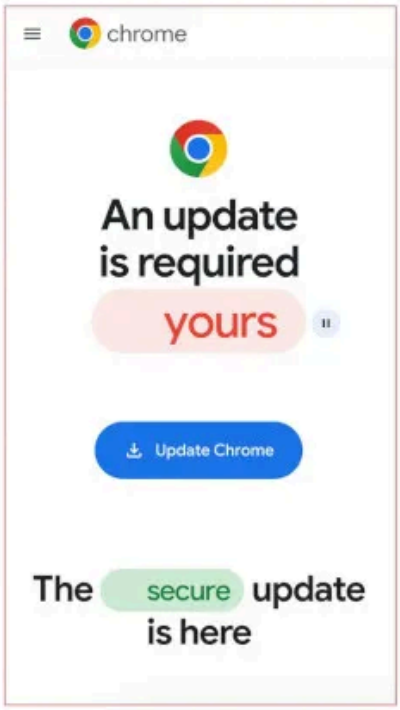
C'est ce qu'on peut lire dans le rapport publié par la firme de cybersécurité ThreatFabric.

Ces derniers ont identifié le logiciel malveillant Brokewell en effectuant des recherches concernant de fausses mises à jour du navigateur Chrome.

On retrouve des annonces et des pages qui tentent de nous faire croire que notre navigateur n'est pas à jour et qu'une mise à jour s'impose.

> « Se faire passer pour une mise à jour du navigateur est une méthode courante utilisée par les cybercriminels pour inciter les victimes à télécharger et à installer des logiciels malveillants », peut-on lire dans le rapport de ThreatFabric.

Ces derniers estiment que cette page en apparence « innocente » va surtout berner les internautes « sans méfiance ».



Voici un exemple de pages web faisant la promotion de fausse mise à jour de Chrome. - *francoischarron.com*

Si on clique sur l'une d'entre, on s'avère à installer Brokewell.
Il s'agit d'un logiciel malveillant de type Cheval de Troie.

Ce dernier serait toujours en cours de développement par ailleurs.
C'est loin d'être rassurant quand on voit déjà les dommages qu'il peut faire.

Nos comptes de banque dans sa ligne de mire... et bien plus!

Une fois téléchargé sur notre téléphone, Brokewell va déployer ses actions malveillantes dans le but d'aller voler notre argent.

Pour ce faire, il va notamment créer de fausses pages de connexion par-dessus celles de nos applications bancaires.

De cette façon, on pense se connecter normalement, mais en réalité on s'avère à donner nos accès aux pirates.
Ces derniers peuvent ensuite aller pêcher allégrement dans notre compte.

Mais Brokewell ne s'arrête pas là.

Il va également agir comme logiciel de capteur de touches.
Ainsi, tout ce qu'on tape, il va l'intercepter.

Tous nos comptes sont alors à risque moindrement qu'on rentre nos informations de connexions.

C'est sans compter toutes les communications que l'on partage avec nos proches ou collègues de travail.

Il peut également activer le micro de notre téléphone et donc enregistrer toutes nos conversations.

Enfin, il peut subtiliser notre emplacement géographique, mais aussi l'historique de nos appels téléphoniques.

Bref, ce logiciel malveillant agit comme véritable logiciel espion et est en mesure de prendre pratiquement l'accès complet de notre appareil.

Fait rare, ThreatFabric croit même savoir exactement qui est derrière celui-ci.

Il s'agirait d'un individu nommé Baron Samedit.
Ce pirate informatique est en quelque sorte un mercenaire, alors qu'il conçoit et offre des solutions malveillantes aux plus offrants.

Comment se protéger de Brokewell?

La première façon de se protéger, c'est de se rappeler qu'on doit toujours faire les mises à jour d'applications Android dans le Play Store de Google.

On ne doit jamais faire une mise à jour via un lien proposé sur une page web ou dans une fenêtre publicitaire.

Enfin, comme on le mentionnait d'entrée de jeu, il est primordial de se munir d'un bon antivirus mobile.

Pour 15-20$ par année, on s'assure de protéger notre appareil et nos données personnelles.

Ces solutions de protection identifient les menaces et les bloquent pour maintenir notre téléphone en sécurité.

Voir nos suggestions d'antivirus mobile

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20240429
"C'est ensemble qu'on avance"