_swissprivacy.law

TikTok : une analyse technique helvétique des risques de sécurité

Pauline Meyer, le 12 septembre 2023

Suite aux interdictions au sein de certaines institutions de l'UE d'utiliser TikTok sur les téléphones professionnels, le nouvel Institut national suisse pour les tests de cybersécurité a publié les résultats de ses tests techniques sur l'application, recommandant de considérer son utilisation avec précaution.

Analyse technique de la sécurité de l'application mobile « TikTok » du 18 avril 2023

Cadre de l'analyse

L'Institut national de test pour la cybersécurité (NTC) est un nouvel institut indépendant actif en Suisse qui se charge de tester la sécurité des produits TIC, sur incitation ou de sa propre initiative.

Il prend l'initiative, après incitation par le Centre national pour la cybersécurité (NCSC), de tester l'application TikTok pour apporter un élément de réponse aux questionnements, sur territoire helvétique, relatifs à l'utilisation de l'application par des employés d'entreprises ou de l'administration. La Commission européenne et le Parlement européen ont décrété début 2023 l'interdiction de l'application sur les appareils professionnels de leur personnel et la Suisse se pose les mêmes questions.

Le NTC publie son analyse à la suite d'une investigation menée par plusieurs experts utilisant l'application dans des conditions réalistes entre le 23 février et le 24 mars 2023. L'étendue de l'investigation, décidée par le NTC, comprend les communications entre l'application et le *back-end* de ByteDance (la société mère de TikTok) ainsi que les autorisations requises par l'application et l'accès à la caméra, au microphone ou encore au GPS des téléphones. Elle ne porte en revanche pas sur le site web de TikTok ou d'autres plateformes, les processus et algorithmes de modération et de censure ou encore les facteurs d'influence psychologiques de l'application. L'exhaustivité de l'analyse technique est par ailleurs limitée par le temps consacré à effectuer les investigations.

Le NTC soulève trois risques prioritaires dans son analyse, ainsi que des risques moyens et faibles.

Risques prioritaires

Les risques prioritaires sont considérés comme tels dans la mesure où ils sont susceptibles d'affecter tous les utilisateurs de l'application et parce que les vulnérabilités sont facilement exploitables.

Le premier risque prioritaire concerne la transmission de valeurs de hachage de contacts à ByteDance. Lorsque des utilisateurs de TikTok autorisent l'application à accéder à leurs contacts, celle-ci transmet directement à ByteDance les valeurs de hachage des numéros de contacts issus du carnet d'adresses des utilisateurs. Bien que les informations ne soient pas en texte clair, le NTC suppose que ByteDance peut les reconstituer à partir des valeurs de hachage. ByteDance peut ensuite les attribuer clairement à une personne, processus effectué sans le consentement ou l'information des personnes concernées.

Le second risque prioritaire porte sur le manque de chiffrement des messages directs ou privés, qui ne sont pas protégés par un chiffrement de bout en bout. Partant, ByteDance, l'opérateur de l'infrastructure (Akamai Technologies) et d'autres acteurs sont susceptibles de lire et de modifier le contenu des messages.

Le dernier risque prioritaire vise l'utilisation des services de localisation au lancement de l'application. TikTok transmet à Bytedance des informations de géolocalisation (en partie chiffrées) concernant des utilisateurs sur iOS lors de chaque démarrage de l'application, à condition que l'utilisateur autorise TikTok à accéder à la localisation durant l'utilisation de l'application. Ces transferts ne semblent pas être nécessaires pour le fonctionnement de l'application et ces informations peuvent servir à créer un profil relatif aux mouvements d'un utilisateur de TikTok.

Risques moyens

Les risques de priorité moyenne impliquent que de nombreux utilisateurs de l'application peuvent être concernés et que les vulnérabilités découvertes sont moins facilement exploitables que pour les risques prioritaires.

Il en va d'une part de la collecte, par TikTok, d'informations sur l'environnement du téléphone ainsi que de leur transmission sur le *back-end* de Bytedance, ce qui permet à l'application de se comporter différemment en fonction de l'environnement. D'autre part, la non-utilisation de méthodes d'authentification multifactorielle est problématique, car il est possible, en cas de compromission de l'unique facteur d'authentification, de prendre le

contrôle du compte.

Risques faibles

Le NTC soulève des risques de priorité faible, car leur exploitation n'est pas susceptible de causer des dommages directs. Leur exploitation permet simplement aux potentiels attaquants de gagner un avantage.

Premièrement, TikTok envoie du contenu au *back-end* ByteDance avec l'utilisation d'en-têtes HTTP non standardisés et partiellement chiffrés sans savoir ce qui est transmis en clair ou non. Malgré l'impossibilité d'examiner les données transmises dans les en-têtes en raison des délais impartis pour l'enquête, le NTC explique qu'il serait en tout cas possible de transmettre discrètement à ByteDance toutes les données auxquelles l'application a accès, à l'instar d'une liste des applications installées sur un système d'exploitation.

Deuxièmement, lorsque TikTok est ouvert, l'application vérifie si certaines applications sont installées sur les smartphones, ce qui peut révéler des informations sur les utilisateurs. Cependant, le NTC ne sait pas si ces informations sont transmises à ByteDance et considère que le risque est faible.

Troisièmement, l'application TikTok envoie toutes les heures des requêtes HTTP à ByteDance lorsqu'elle fonctionne en arrière-plan, ce qui permet à cette dernière (ainsi qu'à Akamai Technologies) de disposer sur la base de l'adresse IP de la localisation imprécise d'un smartphone. Cette information peut être utilisée conjointement à d'autres informations pour créer un profil lié aux mouvements d'un utilisateur.

Quatrièmement, l'application contient un navigateur intégré sur Android, ce qui permet à TikTok de surveiller et de manipuler les entrées et le contenu des utilisateurs dans ce navigateur. Le navigateur n'étant utilisé que dans des scénarios limités, le risque est considéré comme faible par le NTC.

Recommandations

Le NTC recommande une étude plus approfondie pour les informations sur l'environnement des téléphones collectées par TikTok, pour les informations chiffrées transmises par des en-têtes HTTP à ByteDance ou encore pour le contrôle des autres applications ouvertes.

En parallèle, le NTC recommande aux utilisateurs de prendre des précautions avec TikTok en

utilisant le service de messagerie directe uniquement pour du contenu non sensible, en refusant l'accès de l'application aux contacts et aux données de localisation (quitte à les autoriser manuellement pour publier du contenu), en fermant complètement l'application hors utilisation et en privilégiant un navigateur externe.

Conclusion

Au vu des recommandations émises par le NTC, l'on peut se demander quels sont son statut et son mandat. Initialement, la cyberstratégie nationale 2023 percevait la création du NTC comme un complément aux capacités du Cyber-Defence Campus (CYD Campus) pour mener des évaluations indépendantes relatifs aux risques de sécurité inhérents aux produits et services informatiques. Le NTC annonce sur son site web identifier et tester les vulnérabilités de tels produits pour mettre ses résultats à disposition de la population, des pouvoirs publics et des acteurs économiques.

Bien que la création du NTC réserve de nombreuses promesses, tant son mandat que son statut ou son rôle devront être précisés. L'analyse de l'application TikTok soulève des questions quant à l'expertise technique, stratégique, juridique ou éducative du NTC, avec certaines formulations susceptibles d'être hasardeuses, par exemple lorsqu'il est fait mention du niveau de sensibilité de certaines données personnelles. En outre, ses relations avec des autorités comme le NCSC ou les questions en lien avec les résultats fournis à différents destinataires devraient être clarifiées. Le NTC semble principalement s'adresser aux utilisateurs de l'application, sous réserve d'une recommandation, sans destinataire identifiable, visant à réaliser une étude approfondie de TikTok.

Compte tenu de ces observations, l'expertise du NTC est la bienvenue, mais son mandat et son domaine d'expertise doivent être précisés, de même que ses relations, notamment avec l'administration fédérale.

Alors qu'en Suisse l'administration fédérale n'a pas interdit l'utilisation de l'application à ses collaborateurs, TikTok tente de se conformer à certaines obligations en vertu du Règlement sur les services numériques (cf. www.swissprivacy.law/184/). Cependant, des mesures plus radicales d'autres États continuent à être prises (à raison peut-être?), notamment en ce qu'il en va de l'utilisation de celle-ci par les employés administratifs en raison de la relation entre TikTok et sa société mère chinoise ByteDance.

_swissprivacy.law

Proposition de citation : Pauline MEYER, TikTok : une analyse technique helvétique des risques de sécurité, 12 septembre 2023 *in* www.swissprivacy.law/251