Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 01 août 2016
N° CERTFR-2016-ACT-031

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-031

1 - Cyber-risques liés à l'installation et l'usage de l'application Pokémon Go

Lancé courant juillet par la société Niantic, le jeu Pokémon Go est depuis devenu un phénomène de société, au point d'être installé sur plus de 75 millions de terminaux mobiles dans le monde. Certains acteurs malveillants ont rapidement tenté d'exploiter la popularité du jeu à des fins criminelles. Certaines précautions s'imposent donc avant de pouvoir tenter de capturer un Dracaufeu ou un Lippoutou sans porter atteinte à la sécurité de son ordiphone.

Applications malveillantes

Des sociétés spécialisées en sécurité informatique ont mis en évidence la présence de nombreuses fausses applications se faisant passer pour une version officielle du jeu. Ces applications sont susceptibles de naviguer sur des sites pornographiques pour simuler des clics sur des bannières publicitaires, de bloquer l'accès au terminal et de ne le libérer qu'en contrepartie d'une rançon, ou bien même d'installer d'autres codes malveillants. Au vu du nombre d'applications concernées (plus de 215 au 15 juillet 2016), cette technique semble très populaire, en particulier dans les pays où le jeu n'est pas encore disponible via les sites officiels.

Niveau de permissions demandées par l'application

La version initiale du jeu sur iOS présentait un problème au niveau de la gestion des permissions. En effet, le processus d'enregistrement d'un compte Pokemon Go à l'aide d'un compte Google exigeait un accès complet au profil Google de l'utilisateur.

Suite à la prise de conscience [3] de ce problème, la société Niantic a rapidement réagi en précisant qu'il s'agissait d'une erreur lors du développement. Elle propose désormais une mise à jour pour limiter le niveau d'accès requis au profil Google de l'utilisateur. A noter que la version Android du jeu ne semble pas avoir été affectée par ce problème.

Dans le doute, il est toujours possible de révoquer cet accès en se rendant sur la page de gestion des applications autorisées à accéder à son compte Google [4].

Collecte de données personnelles

De par son fonctionnement, l'application collecte en permanence de nombreuses données personnelles qui sont ensuite transmises au développeur du jeu, par exemple les informations d'identité liées au compte Google ou la position du joueur obtenue par GPS. Certaines indications visuelles (nom de rue, panneaux, etc) présentes sur les photos prises avec l'application peuvent aussi fournir des indications sur la position actuelle du joueur. La désactivation du mode "réalité augmentée" lors de la phase de capture permet de se prémunir de ce type de risques (et accessoirement, de réduire l'utilisation de la batterie de l'ordiphone).

Pokemons et BYOD

Il peut être tentant d'utiliser un ordiphone professionnel pour augmenter les chances de capture d'un Ronflex. Même s'il est souvent délicat de répondre par la négative à une requête émanant d'un VIP, il semble peu opportun de déployer ce type d'application dans un environnement professionnel, en raison des différents risques évoqués précédemment.

Recommandations

Le CERT-FR recommande de n'installer que la version originale du jeu présente sur les boutiques d'Apple et de Google (liens [6] et [7]). En complément, il convient de désactiver la possibilité d'installer une application téléchargée depuis un site tiers (sous Android, paramètre "Sources inconnues" du menu "Sécurité").

Il est également conseillé de vérifier les permissions demandées par l'application. La version originale du jeu nécessite uniquement :

- d'accéder à l'appareil photo pour les fonctionnalités de réalité augmentée ;
- de rechercher des comptes déjà présents sur l'appareil ;
- de localiser l'utilisateur grâce au GPS ou aux points d'accès Wi-Fi ;
- d'enregistrer localement des fichiers sur le téléphone.

Toute autre permission peut sembler suspecte et mettre en évidence la présence sur l'ordiphone d'une version altérée de l'application.

Le CERT-FR suggère de mettre en place un cloisonnement entre l'identité réelle du joueur et celle de dresseur Pokémon. Pour cela, il est possible d'ouvrir un compte directement auprès du Club des dresseurs Pokémon [8] ou bien de créer une adresse Gmail dédiée à cet usage.

Enfin, le CERT-FR déconseille de pratiquer cette activité dans des lieux où le geo-tagging du joueur pourrait avoir des conséquences (lieu de travail, sites sensibles, etc) [9].

Documentation

1 Fake Pokemon Go apps lock phones and access porn sites :
http://www.independent.co.uk/life-style/gadgets-and-tech/gaming/fake-pokemon-go-apps-lock-phones-and-access-porn-sites-a7141366.html

2 Pokémon GO hype, first lockscreen tries to catch the trend :
http://www.welivesecurity.com/2016/07/15/pokemon-go-hype-first-lockscreen-tries-catch-trend/

3 Pokemon Go is a huge security risk :
http://adamreeve.tumblr.com/post/147120922009/pokemon-go-is-a-huge-security-risk

4 Autorisations des applications accédant au compte Google :
https://security.google.com/settings/security/permissions

5 Mobilité et BYOD, "Pokémon GO est un cauchemar pour les entreprises" :
http://www.zdnet.fr/actualites/mobilite-et-byod-pokemon-go-est-un-cauchemar-pour-les-entreprises-39840094.htm

6 Version officielle du jeu sur le site Google Play :
https://play.google.com/store/apps/details?id=com.nianticlabs.pokemongo

7 Version officielle du jeu sur le site iTunes :
https://itunes.apple.com/fr/app/pokemon-go/id1094591345

8 Club des dresseurs Pokémon :
https://www.pokemon.com/fr/club-des-dresseurs-pokemon

9 US Government operational security guidance for intelligence officers and friends playing Pokémon GO :
https://twitter.com/RidT/status/754298406034702336

2 - Rappel des avis émis

Dans la période du 25 au 31 juillet 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-250 : Multiples vulnérabilités dans SCADA les produits Siemens
- CERTFR-2016-AVI-251 : Multiples vulnérabilités dans PHP
- CERTFR-2016-AVI-252 : Multiples vulnérabilités dans Xen

– CERTFR-2016-AVI-253 : Vulnérabilité dans Google Chrome
– CERTFR-2016-AVI-254 : Multiples vulnérabilités dans Wireshark
– CERTFR-2016-AVI-255 : Multiples vulnérabilités dans les produits Cisco

Gestion détaillée du document

01 août 2016 version initiale.