TheTruthSpy : cet outil de recherche de logiciels espions indique si votre appareil Android a été compromis

Zack Whittaker
@zackwhittaker /17 août 2022

Une enquête de TechCrunch en février 2022 a révélé qu'une flotte d'applications de logiciels espions grand public, y compris TheTruthSpy, partage une vulnérabilité de sécurité commune qui expose les données personnelles de centaines de milliers d'utilisateurs d'Android.

Notre enquête a trouvé des victimes dans pratiquement tous les pays, avec de grands groupes aux États-Unis, en Europe, au Brésil, en Indonésie et en Inde. Mais la nature furtive des logiciels espions signifie que la plupart des victimes n'auront aucune idée que leur appareil a été compromis à moins qu'elles ne sachent où regarder sur leur appareil .

Puis, en juin, une source a fourni à TechCrunch un cache de fichiers vidé des serveurs du réseau interne de TheTruthSpy.

Le cache comprenait une liste de tous les appareils Android compromis par l'une des applications de logiciels espions du réseau de TheTruthSpy, notamment Copy9, MxSpy, iSpyoo, SecondClone, TheSpyApp, ExactSpy, GuestSpy et FoneTracker. Hormis leurs noms, ces applications sont presque identiques et communiquent toutes avec la même infrastructure de serveur.

La liste contient soit le numéro IMEI, soit l'identifiant publicitaire unique associé à chaque appareil compromis jusqu'en avril 2022, date à laquelle les données ont vraisemblablement été supprimées du réseau interne du logiciel espion. TechCrunch a vérifié l'authenticité de la liste en faisant correspondre les IMEI connus du graveur et des appareils virtuels que nous avons utilisés dans le cadre de notre enquête sur le réseau de logiciels espions.

À l'aide de cette liste d'appareils compromis, TechCrunch a créé un outil de recherche de logiciels espions pour vous permettre de vérifier si votre appareil Android a été compromis par les applications TheTruthSpy et de fournir des ressources pour supprimer les logiciels espions de votre appareil.

Comment fonctionne l'outil de recherche de logiciels espions ?
Avant de commencer, il est important d'avoir un plan de sécurité en place. La Coalition Against Stalkerware et le National Network to End Domestic Violence offrent des conseils et des orientations aux victimes et aux survivants de stalkerware.

C'est ainsi que vous démarrez avec l'outil.

1. Tout d'abord, trouvez un appareil que vous savez sûr, comme le téléphone d'un ami de confiance ou un ordinateur dans une bibliothèque publique.

2. Visitez cette même page Web à partir de cet appareil de confiance : https://techcrunch.com/pages/thetruthspy-investigation/?

3. Entrez le numéro IMEI ou l'identifiant publicitaire de l'appareil que vous soupçonnez d'être compromis dans l'outil de recherche. Vous voudrez peut-être vérifier les deux.

Voici comment vous les trouvez :

Un numéro IMEI est un numéro de 14 à 15 chiffres qui est unique à votre téléphone portable. À partir du pavé numérique de votre téléphone, tapez ✱ #06# et votre numéro IMEI (parfois appelé MEID) devrait apparaître sur votre écran. Vous devrez peut-être appuyer sur le bouton d'appel sur certains modèles de téléphone.

L'identifiant publicitaire de votre appareil se trouve dans Paramètres > Google > Annonces, bien que certaines versions d'Android puissent différer légèrement. Les identifiants publicitaires varient mais comportent généralement 16 ou 32 caractères et sont un mélange de lettres et de chiffres.

Si vous avez réinitialisé ou supprimé, ou si votre identifiant publicitaire a autrement changé depuis l'installation du logiciel espion, cet outil peut ne pas identifier votre appareil comme compromis.

Le numéro IMEI peut être trouvé en composant * # 06 # - ou étoile livre zéro six livres. L'identifiant des annonces de votre appareil peut être trouvé via Paramètres, puis Google, puis Annonces.

Si l'outil de recherche de logiciels espions renvoie une "correspondance", cela signifie que le numéro IMEI ou l'identifiant publicitaire de l'appareil a été trouvé dans la liste divulguée et que l'appareil correspondant a été compromis par l'une des applications de logiciels espions TheTruthSpy au plus tard en avril 2022.

Si vous obtenez une "correspondance probable", cela signifie que votre numéro IMEI ou l'identifiant publicitaire de votre appareil correspond à un enregistrement de la liste, mais que l'entrée peut contenir des données superflues, telles que le nom du fabricant de l'appareil. Ce résultat signifie que l'appareil correspondant a probablement été compromis par l'une des applications TheTruthSpy, mais que vous devez confirmer en vérifiant les signes indiquant que le logiciel espion est installé .

Si "aucune correspondance" n'est trouvée, cela signifie qu'il n'y a pas d'enregistrement correspondant à cet appareil dans la liste des appareils compromis qui a été divulguée. Cela ne signifie pas automatiquement que l'appareil est exempt de logiciels espions. Votre appareil peut avoir été compromis par le logiciel espion après avril 2022, ou avoir été ciblé par un autre type de logiciel espion.

Que dois-je faire maintenant ?
Pour confirmer si un appareil Android est actuellement compromis, vous devez rechercher des signes indiquant que le logiciel espion est installé. Ce guide explique comment rechercher des preuves que votre téléphone a été compromis par un logiciel espion et comment le supprimer de votre téléphone.

Comme le logiciel espion est conçu pour être furtif, n'oubliez pas que sa suppression risque d'alerter la personne qui l'a installé, ce qui pourrait entraîner une situation dangereuse. La Coalition Against Stalkerware et le National Network to End Domestic Violence offrent un soutien, des conseils et des ressources sur la façon de créer un plan de sécurité.

Autres questions :
Que fait cet outil de recherche de logiciels espions ?
Cet outil de recherche vous permet de vérifier si votre appareil Android a été compromis par l'une des applications TheTruthSpy avant avril 2022.

TechCrunch a obtenu une liste contenant le numéro IMEI ou l'identifiant publicitaire unique de l'appareil collecté sur chaque appareil compromis. Chaque téléphone ou tablette connecté à un réseau cellulaire possède un numéro IMEI unique codé en dur dans le matériel de l'appareil, tandis que les identifiants publicitaires sont intégrés dans le logiciel de l'appareil et peuvent être facilement réinitialisés et modifiés par l'utilisateur.

Une fois que le logiciel espion est installé, il renvoie l'un des identifiants du téléphone à ses serveurs, tout comme de nombreuses autres applications le font pour des raisons autorisées comme la publicité, bien que Google ait largement restreint l'accès des développeurs aux numéros IMEI de 2019 en faveur des identifiants publicitaires plus contrôlables par l'utilisateur.

Cet outil de recherche ne stocke pas les numéros IMEI soumis ni les identifiants publicitaires, et aucune donnée n'est donc partagée ou vendue.

Pourquoi TechCrunch a-t-il créé un outil de recherche de logiciels espions ?
La liste ne contient pas suffisamment d'informations pour que TechCrunch puisse identifier personnellement ou avertir les propriétaires d'appareils individuels. Même si c'était le cas, nous ne pourrions pas contacter les victimes de peur d'avertir également la personne qui a installé le logiciel espion et de créer une situation dangereuse.

Un téléphone peut contenir certaines des informations les plus personnelles et les plus sensibles d'une personne. Aucun membre de la société civile ne devrait jamais être soumis à une surveillance aussi invasive à son insu ou sans son consentement. Grâce à cet outil, chacun peut vérifier si ce logiciel espion a compromis son appareil Android à tout moment et en tout lieu, lorsqu'il est sûr.

L'outil de recherche ne peut pas vous dire si votre appareil est actuellement compromis. Il peut seulement vous dire s'il y a une correspondance avec un identifiant d'appareil trouvé dans la liste qui a fuité, ce qui indique que l'appareil a probablement été compromis avant avril 2022.

Que peut faire ce logiciel espion ?
Les applications d'espionnage grand public sont souvent présentées comme des applications de surveillance des enfants, mais ces applications sont également appelées "stalkerware" ou "spouseware" en raison de leur capacité à suivre et à surveiller d'autres personnes, comme les conjoints et les partenaires domestiques, sans leur consentement.

Des applications comme TheTruthSpy sont téléchargées et installées par une personne ayant un accès physique au téléphone d'une personne et sont conçues pour rester cachées des écrans d'accueil, mais elles téléchargeront silencieusement et continuellement les journaux d'appels, les messages texte, les photos, les historiques de navigation, les enregistrements d'appels et les données de localisation en temps réel du téléphone à l'insu de son propriétaire.

Quelle est la faille de sécurité ?
Les neuf applications d'espionnage connues du réseau de TheTruthSpy partagent la même infrastructure, mais en raison d'un codage de mauvaise qualité, elles partagent également la même faille de sécurité. Cette faille, connue officiellement sous le nom de CVE-2022-0732, est simple à exploiter et permet à quiconque d'obtenir à distance un accès quasi illimité aux données de l'appareil de la victime.

Sans espérer que la vulnérabilité soit corrigée, TechCrunch a publié des informations sur le réseau afin d'aider les victimes à identifier et à supprimer le logiciel espion si elles peuvent le faire en toute sécurité.

Les aspects juridiques

Si vous utilisez cet outil de recherche de logiciel espion, TechCrunch recueillera votre numéro IMEI ou votre identifiant publicitaire et votre adresse IP dans le seul but de vous aider à identifier si votre appareil a été compromis par ce logiciel espion. Les numéros IMEI et les identifiants publicitaires ne sont pas stockés, vendus ou partagés avec des tiers et sont supprimés dès que vous recevez les résultats de l'outil de recherche de logiciels espions. Les adresses IP sont brièvement stockées pour limiter les demandes automatisées uniquement. TechCrunch n'est pas responsable des pertes ou dommages causés à votre appareil ou à vos données et n'offre aucune garantie quant à l'exactitude des résultats. Vous utilisez cet outil à vos propres risques.