Ça pourrait être dangereux !

Installation de logiciels espions via des attaques par ingénierie sociale en Italie

Ça pourrait être dangereux ! Installation de logiciels espions via des attaques par ingénierie sociale en Italie

Texte d'origine en italien

Potrebbe essere dannoso!

2025

brughiere.noblogs.org/post/2025/11/12/potrebbe-essere-dannoso

Traduction et mise en page

No Trace Project

notrace.how/resources/fr/#pourrait-etre-dangereux

Note du No Trace Project :

Ce texte décrit comment des camarades Italiens se sont fait piéger et ont installé des logiciels espions sur leurs téléphones suite à des attaques par ingénierie sociale impliquant de faux techniciens qui prétendaient travailler pour des opérateurs de téléphonie mobile. Sur la base de notre expérience et de l'expérience d'autres camarades, nous pensons que les attaques décrites dans ce texte :

- Ont probablement été menées par des acteurs étatiques, peut-être des unités de police locales ou des procureurs.
- Ont très probablement nécessité la collaboration des opérateurs de téléphonie mobile, qui auraient déconnecté et reconnecté la ligne à distance afin que le téléphone semble avoir des problèmes de connexion, permettant au faux technicien d'intervenir de manière crédible.

Ce texte nous rappelle que les capacités de surveillance des autorités répressives sont limitées par leurs ressources, financières et autres. Tandis que les agences de renseignement ont peut-être accès à des logiciels espions plus sophistiqués qui peuvent être installés de manière plus fiable et discrète, les unités de police locales et les procureurs doivent peut-être compter sur des techniques moins sophistiquées.

Cela montre l'importance de sensibiliser aux attaques par ingénierie sociale au sein de nos mouvements, afin d'éviter que d'autres camarades ne se fassent piéger ainsi.

L'utilisation de logiciels espions contre des politiciens, entreprises, avocats et activistes est en augmentation. Nous avons des raisons de penser que des logiciels similaires sont utilisés dans le cadre d'enquêtes contre des invididus associés à certains pans du mouvement. C'est sans doute plus simple pour les procureurs de passer par des start-ups externes pour des logiciels qui, bien que moins sophistiqués et moins chers que Pegasus, Predator, Graphite ou Triangulation, remplissent tout de même leurs rôles d'espions et collectent des informations sur leurs victimes sans leur consentement.

Récemment, des camarades ont subi des intrusions dans leurs appareils mobiles. D'abord, iels ont soudainement et sans raison perdu leur connexion à Internet et aux services de téléphonie. Au même moment, tous les appels sortants ont été redirigés vers la centrale de l'opérateur (ou bien l'opérateur a été contacté pour demander des explications). Après un appel avec un assistant qui, ignorant ou mal informé, diagnostiquait de problables problèmes de connexion, iels ont été immédiatement re-contactés par un différent numéro prétendant être un technicien de l'opérateur de téléphonie.

Le technicien a dit que le téléphone n'était pas à jour. Il a ensuite dicté avec précision et politesse toutes les étapes pour corriger le problème, dont l'installation d'une application comportant le nom et le logo de l'opérateur associé à la carte SIM.

Les étapes d'installation montrent à quel point l'application est intrusive :

- D'abord, l'analyse d'application Play Protect est désectivée au sein du Play Store. Cette fonctionnalité protège l'appareil d'applications potentiellement dangereuses et s'assure que les applications installées sont saines et fiables.
- Un SMS arrive avec un lien vers une page qui ressemble au site web de l'opérateur. On te demande ensuite de cliquer sur un bouton qui ressemble au bouton de Google Play pour télécharger la « mise à jour ».

- Le fichier est téléchargé, outrepassant le Play Store, et ouvert depuis Téléchargements, malgré des avertissements du téléphone qui sont tous ignorés. Pour finaliser l'installation, tu dois changer les paramètres du téléphone pour autoriser l'installation d'applications depuis cette source.
- Les paramètres du téléphone sont ensuite modifiés pour autoriser l'accès au réseau téléphonique, permettant d'utiliser la connexion « données » de l'opérateur pour envoyer et recevoir des informations.
- L'application est autorisée à fonctionner en arrière-plan et à démarrer automatiquement quand le téléphone est allumé. Cela lui permet de continuer de fonctionner même quand elle n'est pas visible sur l'écran.
- Toutes les permissions sont octroyées à l'application, y compris l'accès à la caméra, au microphone, aux contacts, au téléphone, aux SMS, au calendrier, à la géolocalisation, aux fichiers, etc.
- Dans les paramètres, l'optimisation de la batterie est désactivée pour l'application pour que son activité ne soit pas limitée pour conserver de la batterie.
- Le téléphone est redémarré, et une fois redémarré, le symbole du microphone, de couleur verte, est immédiatement apparu dans le coin supérieur gauche. Ensuite il s'est transformé en point vert avant de disparaître.
- Pour couronner le tout, un SMS a été reçu qui demandait « Êtes-vous satisfait de mon service ? »

Après ce processus, il est plausible que toutes les données du téléphone (fichiers, médias, contacts, messages, etc.) étaient transmises à un serveur à distance par l'application espionne installée sous un faux prétexte, transformant le téléphone en un vrai mouchard capable d'activer le microphone, la caméra, et la géolocalisation, ainsi que de prendre des captures d'écran.

Au vu de l'identité des personnes affectées et des capacités des attaquants, il n'est pas difficile d'imaginer l'origine de cette attaque. Nous vous encourageons donc fortement à faire attention aux évènements de ce type, bien que tous les logiciels malveillants ne requièrent pas une installation active par le/la propriétaire du téléphone, comme ça a été le cas ici.

Ce texte décrit comment des camarades Italiens se sont fait piéger et ont installé des logiciels espions sur leurs téléphones suite à des attaques par ingénierie sociale impliquant de faux techniciens qui prétendaient travailler pour des opérateurs de téléphonie mobile.

No Trace Project / Pas de trace, pas de procès. Un ensemble d'outils pour aider les anarchistes et autres rebelles à **comprendre** les capacités de leurs ennemis, **saper** les efforts de surveillance, et au final **agir** sans se faire attraper.

Selon votre contexte, la possession de certains documents peut être criminalisée ou attirer une attention indésirable. Faites attention aux brochures que vous imprimez et à l'endroit où vous les conservez.