Un iPhone éteint peut aussi se faire pirater

DAVID STROM 21 JUIN 2022

Les techniques d'espionnage de nos communications téléphoniques évoluent et nous les combattons chaque jour.

Saviez-vous que même lorsque votre iPhone est éteint, certains de ses composants sont toujours alimentés en énergie ? Des chercheurs ont découvert que c'est l'une des raisons pour lesquelles un nouveau vecteur d'attaque pouvait fonctionner à votre insu. Le problème réside dans le mode économie d'énergie (LPM) de l'iPhone et dans le fait que lorsque cette fonctionnalité est activée, certaines puces de communication continuent de fonctionner. Les fonctionnalités LPM d'Apple ont été introduites lors du lancement de l'iOS 15 et offrent des options comme Localiser Mon iPhone, qui peut continuer à pister et à fonctionner même lorsque le téléphone est éteint.

La fonctionnalité d'un Bluetooth peut devenir le piratage d'un autre

C'est ce qu'ont découvert des chercheurs du laboratoire allemand Secure Mobile Networking Lab de l'Université de technologie de Darmstadt. Ils ont publié un article intitulé

« Evil never sleeps » (Le mal ne dort jamais), dans lequel ils expliquent que l'implémentation du firmware Bluetooth permet aux cybercriminels de créer des malwares qu'il est possible d'exécuter sous certaines conditions. Bien qu'il s'agisse d'une opération complexe en plusieurs étapes, les chercheurs montrent qu'il est, en fait, tout à fait possible d'y parvenir.

Dans leur article, les chercheurs déclarent : « L'implémentation actuelle du mode LPM sur les iPhones d'Apple est opaque et ajoute de nouveaux risques. La conception des caractéristiques LPM semble être principalement motivée par la fonctionnalité, mais elle ne tient pas compte des menaces en dehors des applications prévues. Le fait que l'option Find My Phone continue d'être active alors que l'iPhone est éteint en fait un dispositif de pistage, et son implémentation dans le firmware Bluetooth n'est pas sécurisée contre les manipulations extérieures. »

Ils recommandent à Apple d'inclure un véritable interrupteur matériel de mise sous/hors tension (avec déconnexion complète de la batterie) sur leurs iPhones pour les utilisateurs préoccupés par ce problème. Apple n'a pour l'instant fait aucun commentaire.

L'exploit LPM rappelle deux autres situations qui ont permis à des virus sournois d'infecter vos appareils. Premièrement, le Projet Pegasus de NSO Group, qui utilise un malware qui vient infecter un téléphone cible sans que l'utilisateur ait

besoin de faire quoi que ce soit. L'un de ses vecteurs consiste à exploiter une vulnérabilité dans l'application iMessage d'Apple, par exemple. Il s'agit du spyware (logiciel espion) d'accès à distance qui a été utilisé dans diverses circonstances politiques sensibles, puisque plusieurs chefs d'État ainsi que des journalistes ont été ciblés.

La technique de l'air gap représente un risque

La seconde situation provient de l'exploitation de l'« air gap ». Il s'agit du faux sentiment de sécurité que nous pouvons avoir lorsque nous pensons que nos appareils sont déconnectés de toute connexion Internet ou Wi-Fi. Nous avons évoqué précédemment l'étude menée par des chercheurs du Centre de recherche en cybersécurité de l'université Ben-Gourion en Israël, qui a montré que divers éléments pouvaient être utilisés pour transférer des données de votre téléphone ou de votre ordinateur, notamment les voyants d'accès au disque et les processeurs graphiques (GPU).

Depuis la publication de cette étude, le groupe a identifié une nouvelle méthode d'attaque appelée LANTENNA. Cette attaque consiste à installer sur un ordinateur cible un malware qui encode des signaux de radiofréquence qui sont ensuite transmis via des câbles Ethernet pour contourner les ordinateurs déconnectés selon la technique air gap. Une radio spécialement réglée peut capter ces signaux à l'autre bout de

la pièce et transmettre ensuite les informations à un attaquant. Les chercheurs ont testé deux techniques : ajuster les vitesses de transmission du réseau et générer des signaux utilisant les protocoles UDP pour transporter les données.

Étant donné l'infime probabilité que cet exploit LPM – ou que les compromissions de Pegasus ou de l’air gap – puissent se produire, devons-nous nous inquiéter ? Oui, sans tomber dans la paranoïa. Mieux nous comprenons comment nos ennemis peuvent espionner nos communications téléphoniques, plus nous pouvons avoir confiance dans notre confidentialité et notre capacité à protéger nos communications.

Votre téléphone est sous l'emprise d'un virus.
Rappel, alertez-vous si votre téléphone est anormalement chaud et lent ou que des fenetres ou des applications apparaissent sans votre accord.

Les arnaques par vishing se multiplient et Interpol sévit

Les arnaques par vishing, vocales ou via messagerie, sont en hausse. Interpol sévit, mais vous devez tout de même vous protéger.

Comment devenir un hacker dans le bon sens du terme ?

Découvrez comment Jaya Baloo, directrice des systèmes d'information d'Avast, est devenu une hacker white hat pour contrer les cybercriminels et contribuer à la sécurité d'Internet.

Qu'est-ce qu'un botnet ?
Les botnets sont des réseaux d'ordinateurs et d'appareils sous le contrôle d'un pirate. Découvrez comment fonctionnent les botnets et protégez vos appareils.

Les plus populaires

Les arnaques par vishing se multiplient et Interpol sévit

22 JUIL. 2022
Des comptes Instagram piratés escroquent les utilisateurs

19 JUIL. 2022
Comment devenir un hacker dans le bon sens du terme ?

29 JUIN 2022
Pourquoi est-ce que tout le monde se fait pirater sur Facebook ?

29 JUIN 2022