Apple victime d’une attaque « zéro-clic »

Description

En septembre 2021, Apple a corrigé une faille de sécurité ayant permis au logiciel espion Pegasus, développé par la société de « sécurité » informatique israélienne NSO Group, d’infecter des iPhone et des iPad ciblés par une attaque dite « zéro-clic ».

Alors que les logiciels espions « traditionnels » nécessitent que la personne visée par ce type d’attaque télécharge un document ou clique sur un lien pour installer le programme malveillant sur son téléphone, les logiciels espions dits « zéro-clic » n’ont besoin d’aucune action de la part de l’utilisateur pour infecter un appareil.

Ce type d’attaque, parmi les plus sophistiquées au monde, vise en particulier les services de messagerie instantanée comme WhatsApp, victime du même logiciel espion en mai 2019, et plus récemment iMessage, développée par la firme de Cupertino. Ce piratage est d’autant plus inquiétant qu’il affecte non seulement les dernières versions du système d’exploitation des appareils mobiles d’Apple, iOS 14.4 et iOS 14.6, mis à jour en mai 2021, mais il contourne également une nouvelle fonction de sécurité logicielle intégrée depuis les premières versions d’iOS 14, nommée BlastDoor, censée prévenir ce type de piratage en filtrant les données malveillantes envoyées par l’application iMessage. Cette attaque exploite une vulnérabilité dite *« zero day »*, c’est-à-dire que la faille de sécurité n’a pas fait l’objet d’une publication ou d’un correctif lorsqu’elle est découverte.

Citizen Lab, laboratoire interdisciplinaire de la Munk School à l’Université de Toronto, au Canada, a identifié neuf militants bahreïnis dont les iPhones ont été piratés avec succès entre juin 2020 et février 2021 par l’intermédiaire de deux « exploits », Kismet datant de 2020 et ForcedEntry datant de 2021, c’est-à-dire des éléments de programme qui « exploitent » une faille de sécurité informatique afin de pénétrer et d’utiliser le système d’exploitation des appareils attaqués. Les chercheurs du Citizen Lab avaient également été les premiers à révéler, en août 2016, que le militant émirati des droits de l’homme Ahmed Mansoor avait été ciblé par le logiciel espion Pegasus.

L’exploit « zéro-clic » ForcedEntry utilise un bug dans la fonction d’affichage des images des systèmes d’exploitation d’Apple et infecte le service de messagerie instantanée iMessage afin d’installer discrètement le logiciel espion Pegasus. Une fois l’appareil infecté, le téléphone de la victime devient un véritable mouchard et permet au commanditaire de l’attaque d’accéder aux SMS et messages envoyés et reçus, qu’ils soient ou non cryptés, ainsi qu’au carnet d’adresses de la victime. Pegasus permet également d’activer à distance le micro ou la caméra, d’enregistrer tous les caractères saisis sur le téléphone, d’enregistrer les appels téléphoniques, de photographier l’écran et de capter toutes les données de localisation GPS pour

retracer les déplacements de la victime. Il donne en outre accès à tous les contenus et publications des réseaux sociaux et il peut capter les données des autres applications du téléphone comme WhatsApp, Skype, Facebook ou encore Gmail.

Apple, qui se présente en *« leader en matière de confidentialité »* s'est empressé d'apporter un correctif. Ivan Krstic, le responsable de l'ingénierie et de l'architecture de sécurité d'Apple, a tenté de minimiser l'incident en déclarant, dans un communiqué de presse, que *« les attaques comme celles décrites sont très sophistiquées, coûtent des millions de dollars à développer, ont souvent une courte durée de vie et sont utilisées pour cibler des individus spécifiques.* […] *Bien que cela signifie qu'elles ne constituent pas une menace pour l'écrasante majorité de nos utilisateurs, nous continuons à travailler sans relâche pour défendre tous nos clients ».*

Installée à proximité de Tel Aviv, NSO Group présente tous les atours d'une entreprise de sécurité informatique dont les programmes sont destinés à lutter contre le terrorisme et le crime organisé. Mais cette société israélienne vend également son logiciel espion à des États peu scrupuleux, parmi lesquels figurent notamment l'Espagne, l'Arabie saoudite, l'Azerbaïdjan, Bahreïn, les Émirats arabes unis, la Hongrie, l'Inde, le Kazakhstan, le Maroc, le Mexique, le Panama, le Rwanda ou encore le Togo. Ces gouvernements s'en servent pour espionner des opposants politiques, des militants des droits de l'homme, des journalistes, voire des juges. Même si NSO Group, valorisée plus de 1 milliard de dollars, se fait discrète quant à ses résultats financiers, l'affaire semble rentable. Selon le *Financial Times*, l'entreprise réalisait 208 millions de dollars de chiffre d'affaires en 2018, dont les deux tiers proviennent de la commercialisation du logiciel Pegasus. D'après le média d'information britannique qui a interviewé un homme d'affaires impliqué dans la vente du logiciel Pegasus à l'Arabie saoudite, les Saoudiens auraient déboursé 55 millions de dollars en 2017 pour espionner simultanément 150 personnes.

Puisque le logiciel Pegasus exploite les failles de sécurité « zero day » sur les logiciels de messagerie déployés par les géants du web, son fonctionnement technique évolue en permanence. Dès lors qu'une faille est identifiée par ces sociétés informatiques peu scrupuleuses, elle est exploitée et vendue au plus offrant, le temps que des experts en sécurité l'identifient à leur tour et en fassent l'annonce afin qu'elle soit corrigée. Un jeu du chat et de la souris qui ne semble pas près de s'arrêter.

Sources :

- « Israel's NSO : the business of spying on your iPhone », Mehul Srivastava, Robert Smith, ft.com, May 14, 2019.
- « Forensic Methodology Report : How to catch NSO Group's Pegasus », amnesty.org, July 18, 2021.
- « From Pearl to Pegasus Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits », Bill Marczak, Ali Abdulemam, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, John Scott-Railton, Ron Deibert, Citizen Lab, August 24, 2021.
- « A new NSO zero-click attack evades Apple's iPhone security protections, says Citizen Lab », Zack Whittaker, techcrunch.com, August 24, 2021.
- « The Stealthy iPhone Hacks That Apple Still Can't Stop », Lily Hay, wired.com, August 25, 2021.

- « Pegasus : nouvelle faille zero-day et zero-click dans iMessage, un revers pour Apple », Gilbert Kallenborn, 01net.com, 26 août 2021.

Categorie

1. Techniques

date créée
novembre 2021
Auteur
jacquesandrefines