UN VIRUS CAPABLE DE SURVEILLER LES IPHONE DE «POPULATIONS ENTIÈRES» A ÉTÉ DÉCOUVERT

Il suffisait de visiter, depuis son iPhone, un site Web infecté. En quelques secondes, tous les secrets qu'il renfermait étaient éventés, copiés par un virus informatique sans que l'on remarque rien. Messages, photos, localisation, pas grand-chose n'échappait à ce logiciel malveillant découvert par les chercheurs en sécurité informatique de Google.

Leur découverte est en effet déroutante. D'abord, le virus met en œuvre 14 vulnérabilités dans le logiciel qui équipe téléphones mobiles et tablettes d'Apple, pourtant considéré comme bien sécurisé. Selon les chercheurs de Google, le virus a été actif pendant plus de deux ans, à partir de 2016, Le virus était parfaitement efficace, y compris sur les tout derniers modèles d'iPhone, équipés de la plus récente mouture d'iOS. S'il suffit aujourd'hui de mettre à jour son téléphone, il était à l'époque impossible de s'en protéger.

D'autant plus que le vecteur d'infection était particulièrement furtif: il suffisait à un utilisateur d'iPhone de se rendre sur un site Web pour que, sans intervention supplémentaire de sa part, le virus pénètre dans son téléphone. Une fois à l'intérieur, ce dernier s'intéressait immédiatement aux archives des messages envoyés et reçus par l'utilisateur à travers les principales applications de messagerie, comme WhatsApp, Telegram, Gmail ou iMessage (le système de SMS d'Apple).

La plupart de ces applications chiffrent les échanges, les rendant impossibles à lire s'ils sont interceptés. Mais le virus permettait de contourner cette difficulté, puisqu'il s'en prenait aux messages stockés sur le téléphone, où ils sont dépourvus de cette protection. Le programme malveillant avait aussi accès à la géolocalisation en temps réel de l'utilisateur infecté, à ses photographies ainsi qu'à son répertoire téléphonique. Enfin, les pirates pouvaient récupérer les mots de passe et les identifiants enregistrés dans le téléphone (qui permettent par exemple d'ouvrir son compte e-mail sans avoir à saisir à chaque fois son mot de passe).

Combien de victimes ce logiciel a-t-il fait? Ian Beer, l'auteur des travaux sur le virus, évoque «des populations entières». Il écrit aussi que les sites distribuant le programme malveillant «reçoivent des milliers de visites par semaine». Le nombre de victimes serait donc très important. Le chercheur se contente d'écrire que les pirates seraient «un groupe se donnant beaucoup de mal pour pirater les utilisateurs d'iPhone dans certaines communautés». Plus loin, avec des mots choisis et sans qu'il soit certain qu'il fasse directement référence au virus qu'ils ont découvert, il explique que pour «être ciblé, il suffit peut-être d'être né dans une certaine région ou de faire partie d'un certain groupe ethnique». Google a également gardé secrète l'adresse IP – l'équivalent de l'adresse postale – vers laquelle étaient redirigées les informations soustraites aux victimes, une information cruciale pour tenter de remonter à l'identité des responsables.