Des fausses antennes radio diffusent des malwares Android en Chine

Les investissements des pirates pour mettre en œuvre leurs attaques sont montés d'un cran en Chine. Les chercheurs de Tencent Security viennent de découvrir l'usage des fausses stations de base radio pour diffuser un malware Android. C'est la première fois que des équipements de réseau mobile sont utilisés pour infecter les smartphones des utilisateurs. Une technique infectieuse qu'avait évoquée Avast dès 2014 et qui devient réalité.

Le groupe de pirate intercepte la communication d'un terminal et de son réseau sans fil d'abonné en se faisant passer pour un opérateur légitime auprès des utilisateurs. La plupart des faux messages reçus émanaient en apparence de Chinal Mobile et China Unicom, les deuxième et troisième opérateurs du pays respectivement. Une fois le réseau usurpé, la méthodologie d'infection est simple. L'utilisateur reçoit un SMS qui invite l'utilisateur à télécharger une application Android, ou une mise à jour, en cliquant sur un lien de téléchargement d'un fichier APK. Ce mode d'installation des applications Android est courant en Chine alors que le Play Store légitime de Google n'y est pas autorisé.

Swearing vole les données personnelles

Le malware en question a été baptisé Swearing (jurer) en raison de la présence de nombreux termes injurieux retrouvés dans son code. Swearing est un trojan qui collecte des données personnelles du terminal, y compris les identifiants et mots de passe. Il est aussi en mesure de contourner les authentifications à deux facteurs utilisées par les services bancaires pour valider une transaction. *« En remplaçant l'application Android SMS originale par une version modifiée, le trojan Swearing peut intercepter les SMS entrants, rendant inutile l'authentification à deux facteurs »*, explique le fournisseur de solutions de sécurité Check Point.

Swearing peut aussi se propager en s'auto-envoyant par SMS aux contacts du carnet d'adresse de la victime. D'autres méthodes pour convaincre les victimes d'installer Swearing sont également utilisées comme un lien vers un fichier bureautique en provenance d'un supérieur demandant sa mise à jour, ou encore vers une vidéo vers un événement mémorable ou une photo d'un-e époux-se infidèl-e, ou encore la classique mise à jour applicative critique réclamée par un opérateur télécom ou une banque.

Des SMS au lieu d'un serveur de commande et contrôle

Le mode de fonctionnement du malware constitue une autre originalité. Il n'est pas piloté par un serveur de commande et contrôle (CC) mais renvoie les données collectées à l'attaquant par le biais d'un SMS ou d'un e-mail. *« Cela permet au logiciel malveillant de couvrir ses communications et de tenter de détecter toute autre activité malveillante »*, commente Check Point.

Si les autorités chinoises ont déclaré avoir arrêté plusieurs membres du groupe créateur de Swearing, Check Point constate que ce dernier continue à sévir. *« Il est donc possible que les attaquants en détention n'étaient qu'une partie d'une opération plus importante pour répandre le malware »*, suggère l'éditeur de sécurité. Pour lutter contre ce fléaux, le gouvernement a renforcé la législation le 1er septembre dernier en imposant la mise en place d'un identifiant unique que les abonnés doivent communiquer à leur opérateur mobile. Si l'abonné ne fournit pas cet identifiant quand il lui est demandé dans une période donnée, l'opérateur doit fermer sa ligne. Radical pour empêcher la propagation du malware par SMS. Mais pas par e-mail, comme a pu le constater Check Point début mars. Swearing ne sera donc pas facile à éradiquer.

Risque de propagation internationale

Il pourrait même se propager hors de Chine. *« La diffusion du cheval de Troie Swearing a été obtenue en utilisant de fausses BTS (stations radio, NDLR) et des SMS automatisés. Ces deux méthodes peuvent également être adoptées par les logiciels malveillants en Occident »*, prévient l'éditeur de sécurité. Surtout s'il n'est pas nécessaire de créer les stations de base mais de prendre celles en service. En août dernier, la société de recherche en faille de sécurité Zimperium relevait plusieurs vulnérabilités du protocole GSM qui permettent à un attaquant de compromettre une station radio et interférer avec les communications légitime de l'opérateur. Du pain béni pour les cyber-attaquants qui y parviendront.

Lire également
Switcher, le malware Android qui s'attaque aux réseaux Wifi
DressCode sur Android taille un costume aux réseaux d'entreprises
Le malware bancaire Dridex devient hyper furtif, grâce au AtomBombing