Télégrammes : iBackdoor sur apps iOS, Câbles USB Type-C défaillants, un DDoS de 320 heures, processeurs Google en vue ?

- **Un malware nommé iBackdoor a été découvert dans plusieurs milliers d'applications iOS.** Des chercheurs de FireEye ont identifié 2846 applications sur l'OS mobile d'Apple corrompues par un malware au sein de mobiSage SDK édité par la société chinoise AdSage. Ce logiciel malveillant baptisé iBackdoor utilise un code javascript entre le smartphone et le serveur de publicité d'AdSage. Grâce à cette porte ouverte, les cybercriminels peuvent procéder à plusieurs actions allant de la capture audio et vidéo à l'insu de l'utilisateur, le traçage de l'utilisateur par la géolocalisation du terminal, la modification des fichiers de données de l'application infectée, le chiffrement des données exfiltré, etc. Une découverte qui intervient au moment où le malware XcodeGhost refait surface en ciblant les entreprises américaines.
- **Les câbles USB Type-C ne sont pas tous de même qualité.** C'est l'expérience qu'à menée un ingénieur de Google en testant les câbles USB Type-C pour le Chrome Pixel. Il a donc mené un comparatif en achetant sur Amazon différents câbles de marque et bon marché. Après plusieurs tests, il s'est aperçu que les connectiques bas de gamme ne répondaient pas aux spécifications de l'USB Type-C et certains étaient même dangereux pour les terminaux. Il pointe du doigt en particulier les résistances internes trop faibles. Elles sont suffisantes pour recharger un smartphone, mais pas pour un ChromeBook plus gourmand en énergie. Pour lui, il faut mieux miser sur des marques connues, Belkin, iOrange-E et Frieq ont ses préférences.
- **Une attaque DDoS de 320 heures.** Au 3e trimestre, les entreprises de 79 pays ont été victimes d'attaques DDoS, a constaté Kaspersky Lab. Mais 91,6% de ces attaques se concentrent dans 10 pays. Au premier rang desquels la Chine (pour 34,5% des attaques par déni de service distribué), suivi des Etats-Unis (20,8%) et la Corée (17,7%) figurent toujours en tête d'un trimestre à l'autre. En dixième position, la France concentre 1,1% des attaques (contre 2,8% au 2e trimestre. Si les frappes durent moins de 24 heures dans 90% des cas, l'éditeur de sécurité a constaté une attaque de plus de 13 jours (320 heures) d'affilé. Et constate une nette progression des charges de plus de 150 heures. 45,6% des attaques enregistrées ont été émises à partir de botnets sous Linux victimes de protections insuffisantes. Un serveur situé au Pays-Bas a subi 22 attaques. Un record sur une même cible sur la période. Les détails sont publiés sur Viruslist.
- **Bientôt des processeurs Google ?** Google va-t-il suivre le chemin d'Apple. Il semble que l'entreprise de Mountain View ait l'intention de concevoir ses propres CPU pour terminaux mobiles à l'image de l'Ax pour l'iPhone. Selon l'annonce publiée fin octobre, Google recherche des ingénieurs capables, notamment, de *« proposer une architecture de puce selon des exigences produit »*. D'autre part, la firme californienne serait en discussion avec plusieurs fondeurs pour produire sa future puce dédiée à son OS mobile, selon *The Information*. Une stratégie pour réduire la fragmentation d'Android ?

Crédit Photo : Juefraphoto-Shutterstock