Wikileaks révèle comment la CIA a piraté des MacBook et iPhone neufs

Wikileaks révèle comment la CIA a piraté des MacBook et iPhone neufs

L'organisation fondée par Julian Assange publie un second corpus de documents présentés comme émanant de la CIA qui décrivent les méthodes de l'agence pour pirater des ordinateurs Apple et des iPhone.

Wikileaks remet le couvert. Près de deux semaines après avoir mis en ligne « Vault 7, Year Zero », un ensemble de plusieurs milliers de documents internes détaillant des dizaines de programmes d'espionnage électronique et informatique de la CIA, l'organisation fondée par Julian Assange a publié une deuxième vague d'archives décrivant les techniques utilisées par l'agence du renseignement extérieur américain pour pirater des produits Apple. Baptisé « Dark Matter », ce second volet explique comment la CIA peut pirater un ordinateur Apple, même si son propriétaire y installe un nouveau système d'exploitation, ou un iPhone neuf en pénétrant le réseau d'approvisionnement et de distribution de la marque à la pomme.
• Wikileaks : 5 questions pour comprendre les dernières révélations

Un logiciel indétectable et impossible à effacer

Selon les documents dévoilés par Wikileaks, la CIA a développé un outil en 2012 nommé « Sonic Screwdriver » permettant de passer outre le processus de démarrage d'un MacBook à partir des accessoires périphériques comme une clé USB ou un adaptateur Ethernet branché dans le port Thunderbolt. L'agence pouvait alors **introduire un micro indétectable dans le logiciel profond** (firmware) de l'ordinateur et **bénéficier d'un accès permanent à son contenu** car même une réinstallation du système d'exploitation ou un reformatage de l'appareil ne pouvait suffire à l'effacer. La CIA devait avoir accès physiquement aux appareils visés pour les infecter.
Un autre document montre que la CIA avait conçu cet outil dès 2008 pour l'installer physiquement sur des iPhone neufs. Selon Wikileaks, il est par conséquent « probable que beaucoup d'attaques physiques par la CIA aient infecté la chaîne d'approvisionnement » d'Apple « en bloquant des commandes ou des livraisons ». L'agence américaine « peut faire cadeau à une cible d'un MacBook Air sur lequel a été installé ce micro », indique un document daté de 2009. « L'outil prendra la forme d'un implant/relais opérant dans le (logiciel) profond du MacBook Air et nous permettant d'avoir les moyens de (le) commander et de (le) contrôler », peut-on lire dans ces documents.

Les produits actuels vraisemblablement pas concernés

Apple n'a pas encore réagi à ces révélations. La plupart des documents datant de plus de sept ans et concernent les premières générations d'iPhone. Il apparaît peu probable que les produits actuels du groupe soient vulnérables à ces techniques. La méthode « Sonic Screwdriver » utilisée pour infecter des MacBook rappelle la faille « Thunderstrike » découverte fin 2014, qui permettait de contaminer un Mac lors de l'allumage à l'aide d'un appareil Thunderbolt vérolé, et corrigée par Apple depuis.
Le 9 mars, Wikileaks avait déjà diffusé près de 9.000 fichiers mettant à nu les capacités d'espionnage de la CIA et le recours à des pratiques particulièrement intrusives pour transformer des télévisions et des voitures connectées en mouchards, espionner des iPhone et des smartphones Android ou contourner des antivirus commerciaux. La CIA n'a jamais authentifié les documents mais de nombreux experts les jugent crédibles. Apple avait fait savoir qu'elle avait corrigé les failles évoquées dans ces documents. Wikileaks affirme détenir des informations sur plus de 500 programmes au total et promet de les publier dans les prochaines semaines.
Benjamin Hue, Journaliste RTL

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DIRTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Wikileaks montre comment la CIA a piraté des MacBook et iPhone neufs*