efcse.eu

Extraits d'actualité cyber…

Auteur : Secrétariat Général EFCSE
17 août 2018

Voici quelques extraits d'actualité cyber, mais surtout, matière à réflexion pour utiliser peut être avec plus de prudence, ordinateurs, smartphones et tablettes qui nous ouvrent au quotidien des possibilités de connexions et d'accès permanents à des informations et à de nouveaux territoires qui semblent sans limite.

A méditer pour anticiper …

Sachez que l'email reste actuellement le vecteur de cyberattaque le plus utilisé, que le facteur humain est le point faible majeur dans le cadre de la cybersécurité, que les objets connectés représentent un terrain de jeu exponentiel pour les cyberpirates et que les robots influenceurs (botnets[1] dits bots) sur les réseaux sociaux ne sont pas tous bienveillants, certains représentent une menace non négligeable par leur action d'influence artificielle sur les opinions.

Le malware Anubis est de retour

Il semble que le malware nommé Anubis soit de retour dans Google Play Store, il aspire mot de passe, coordonnées bancaires et données personnelles.

Google et la société Sophos, société anglaise d'applications de sécurité, travaillent de concert pour limiter les préjudices, ils considèrent que des victimes sont déjà recensées dans environ une trentaine de pays, dont en Europe.

Comme pour tous les rançongiciels, les pirates qui l'utilisent encryptent les fichiers et demandent une rançon pour les libérer, généralement même si l'on s'acquitte de celle-ci il y a peu de chance de récupérer ses fichiers.

Une fois le problème détecté, le plus simple est de restaurer le système à partir d'une sauvegarde et de jouer de prudence à l'avenir avec les régles de base : sauvegardes fréquentes, pas d'ouverture d'email dont l'adresse de l'expéditeur parait douteuse, pas d'ouverture de pièces jointes suspectes (.SCR ou .CAB par exemple), utilisation d'un antivirus à jour, pas de navigation sur internet à partir d'un profil administrateur, etc…

Piratage informatique d'Apple Inc

Un australien âgé de 16 ans est parvenu, pendant près d'un an, à infiltrer le réseau informatique d'Apple, il a pu accéder aux comptes clients de l'entreprise et a téléchargé 90 giga-octets (230 octets) de fichiers sécurisés. Après comparution devant le tribunal pour enfants de Victoria, le verdict est prévu en septembre.

[1] Botnet : contraction en anglais de « robot" et "network"

Cyberattaque

L'une des plus importantes fonderies d'électronique au monde, l'entreprise taïwanaise Taiwan Semiconductor Manufacturing Company [TSMC], a subi une cyberattaque début août ce qui a perturbé ses usines et arrêté une partie de ses lignes de production durant tout un week-end, le temps de rétablir les équipements touchés. Fournisseur de grandes entreprises telles que Apple, AMD, Nvidia et Qualcomm, TSMC a un rôle fondamental dans la production d'appareils électroniques grand public.

Faille de sécurité ?

WhatsApp utilise une paire de clefs de chiffrement pour chiffrer les communications qui a résisté à l'attaque de la société de sécurité Checkpoint dans sa recherche de failles de sécurité.

Cette dernière n'en reste pas moins active pour poursuivre ses opérations de recherche et de test, notamment pour ce qui touche le détournement de message et la manipulation de l'affichage qui restent tout à fait envisageables bien que théorique pour le moment, pour un attaquant chevronné.

Objets connectés et connexion Bluetooth défaillante

De nombreux appareils connectés, dans tous les domaines sont équipés d'un protocole Bluetooth, un défaut dans celui-ci peut permettre la prise de contrôle à distance de l'appareil, cela sans que l'utilisateur s'en rende compte.

Cette option vient d'un défaut sur un type de protocole Bluetooth dit BLE (Bluetooth Low Energy), de basse consommation, ce qui correspond par exemple à une méthode de connexion utilisée par les objets connectés n'ayant pas nécessité à transmettre un gros volume d'informations et devant minimiser leur consommation électrique.

Des attaques pouvant être très fâcheuses notamment dans le domaine médical mais aussi tout simplement avec les montres connectées qui gèrent pas mal de données personnelles. La condition qui, à ce jour, représente l'obstacle majeur pour les pirates est que l'attaque doit être lancée à proximité immédiate de l'objet connecté (20 m maximum).

A propos du « Cryptojacking »

Sachant que les monnaies dites virtuelles c'est-à-dire les cryptomonnaies (fondées sur les principes de la cryptographie) ; sont générées par des ordinateurs effectuant des opérations complexes, un utilisateur lambda consultant une page web peut, à son insu, être générateur de cryptomonnaie.

Le principe est simple, c'est l'exécution d'un script pendant la consultation de la page web, souvent via des sites de partages de fichiers ou de streaming vidéo. Cela a pour effet de ralentir sensiblement la vitesse de l'ordinateur puisque son processeur est occupé à calculer ou plus exactement à « miner » pour le compte de pirates.

Pour vérifier si l'ordinateur est en train de miner il suffit d'aller vérifier l'activité en cours de son processeur (sur PC par exemple via le gestionnaire des tâches dans l'onglet performance). Il est possible de se protéger du minage pirate en

téléchargeant des bloqueurs publicitaires qui agissent également sur les actions de minage puisqu'ils utilisent le même type de code, en conséquence les affichages publicitaires seront aussi bloqués.

Générer de la cryptomonnaie nécessite beaucoup de ressources, les ordinateurs de nombreux usagers du web représentent ainsi une manne pour les pirates qui jouent en arrière plan de la navigation un cryptojacking qui pourrait devenir très rémunérateur, nous n'en sommes qu'à l'émergence de cette nouvelle forme de vol bien plus subtil que le ransomware.