3 - 9 décembre 2018

RAPPORT THREAT INTELLIGENCE

PRINCIPALES FAILLES ET ATTAQUES

- Signet Jewelers, le plus grand détaillant au monde de bijoux en diamants, a corrigé un bug conséquent qui permettait au public d'accéder aux données des clients, y compris leurs adresses de facturation et de livraison, leur numéro de téléphone, leur adresse électronique, les articles achetés et les quatre derniers chiffres de leur numéro de carte bancaire.

- Les banques d'Europe de l'Est sont les cibles principales d'une nouvelle campagne baptisée DarkVishnya, reposant sur la connexion directe d'un appareil amovible au réseau ciblé. L'appareil est connecté par un pirate se faisant passer pour un visiteur. Des ordinateurs portables bon marché et Bash Bunny, un outil d'attaque USB, sont utilisés pour ce faire.

  La blade Check Point Anti-Virus offre une protection contre cette menace (RemoteAdmin.Win32.DameWare).

- Le pirate à l'origine des vastes campagnes du logiciel malveillant bancaire Dridex et du logiciel rançonneur Locky a lancé une campagne d'emailing ciblant de grandes chaînes de vente au détail, de restauration et d'épicerie. La campagne utilise des pièces jointes personnalisées, adaptées à l'entité ciblée.

  Les blades Check Point SandBlast et Anti-Bot offrent une protection contre cette menace (Trojan.Win32.Dridex, Trojan-Ransom.Win32.Locky).

- DanaBot, un cheval de Troie bancaire ciblant des internautes australiens, a récemment changé d'objectif pour se lancer dans la diffusion d'emails de spam. Le logiciel malveillant recueille les identifiants de comptes de messagerie afin d'envoyer des contenus de spam à partir des boîtes de messagerie compromises en tant que réponses aux messages de la boîte de réception.

  Les blades Check Point SandBlast et Anti-Bot offrent une protection contre cette menace (Trojan-banker.Win32.Danabot).

- Un nouveau logiciel malveillant hybride ciblant les ordinateurs Mac a été découvert. Il est diffusé via une fausse version d'Adobe Zii, un logiciel utilisé pour activer les programmes Adobe piratés. Le logiciel malveillant comprend des outils open source, l'extracteur de cryptomonnaie XMRig et la porte dérobée EmPyre.

  Les blades Check Point Anti-Virus et Anti-Bot offrent une protection contre cette menace (Trojan.WIN32.XMRig, Backdoor.Win32.EmPyre).

VULNÉRABILITÉS ET CORRECTIFS

- Une nouvelle vulnérabilité zero-day dans Adobe Flash Player a récemment été utilisée lors d'une attaque ciblée contre un centre de recherche russe. La vulnérabilité, référencée CVE-2018-15982, a été exploitée via un questionnaire Word avec un objet Flash intégré, et a été livrée dans une archive WinRAR.

- Un chercheur a publié une exploitation d'une vulnérabilité de WebKit, le moteur du navigateur Web Safari et d'autres applications Apple. La vulnérabilité tire parti d'une erreur d'optimisation menant à l'exécution de code arbitraire sur les appareils vulnérables. Elle touche les versions iOS et MacOS du navigateur Safari.

- Des pirates ont récemment utilisé une vulnérabilité dans le navigateur Mozilla Firefox qui avait été signalée pour la première fois en 2007. Le bug conduit à l'apparition d'une boîte de dialogue d'authentification en boucle, empêchant les utilisateurs de quitter le site. Les pirates l'utilisent pour forcer les victimes à acheter des produits et des services douteux.

- Apple a publié une mise à jour de sécurité pour plusieurs produits, notamment iTunes, iCloud et la dernière version iOS, 12.1.1. La mise à jour contient des correctifs pour les vulnérabilités d'exécution de code à distance et d'élévation des privilèges, notamment un correctif pour un bug permettant l'accès aux contacts d'un utilisateur d'iPhone lorsque l'appareil est verrouillé.

RAPPORTS ET MENACES

- Des chercheurs de Check Point ont découvert un nouveau service dans le paysage des logiciels rançonneurs. Une entreprise russe nommée « Dr. Shifro » prétend légitimement fournir un service de déchiffrement de fichiers aux victimes de logiciels rançonneurs, alors qu'en réalité, elle paye les auteurs des logiciels rançonneurs et en répercute le coût sur les victimes avec une forte marge bénéficiaire.

- Un rapport analyse plusieurs menaces parmi les plus importantes qui dominent le paysage actuel des menaces, notamment les logiciels malveillants bancaires Emotet et Trickbot, et les attaques PowerShell. Le rapport couvre la diffusion, les fonctionnalités clés et l'évolution attendue de ces menaces.

- Des chercheurs ont examiné les menaces et les méthodes d'attaque les plus couramment utilisées par les cybercriminels durant la saison des fêtes en Occident, notamment les fraudes aux cartes-cadeaux par email, les logiciels malveillants pour terminaux de point de vente et les escroqueries sur les réseaux sociaux.
- Selon un rapport annuel, le paysage des menaces en 2018 a été dominé par des groupes et des pirates exerçant depuis on bon moment. Le célèbre groupe russophone Sofacy qui s'est distingué par des campagnes ciblant les ambassades et les agences de l'UE, ainsi que de nouveaux groupes, notamment, Domestic Kitten en Iran, ciblant principalement des entités au Moyen-Orient et en Asie du Sud-Est.
- Le formjacking est une technique utilisée pour dérober les informations relatives au paiement sur les pages web de paiement des portails de commerce électronique via du code JavaScript.

  Les blades Check Point Anti-Bot et Anti-Virus offrent une protection contre cette menace (Magecart).