10 - 16 décembre 2018

RAPPORT THREAT INTELLIGENCE

PRINCIPALES FAILLES ET ATTAQUES

- Des informations confidentielles sur 120 millions de Brésiliens ont été exposées en ligne en raison d'une mauvaise configuration d'un serveur de sauvegarde. Les détails comprennent les numéros d'identification de contribuable qui sont associés à leur historique de débit et de crédit bancaire, l'historique de vote, le nom complet, les adresses email, les numéros de téléphone, etc.

- Des chercheurs ont mis au jour les nombreuses activités du groupe de cyberespionnage SeedWorm. Le groupe a lancé de nouvelles variantes de ses outils pour cibler 131 victimes, principalement dans les secteurs des télécommunications et des services informatiques, probablement pour fournir un accès à ses clients.

  La blade Check Point Anti-Virus offre une protection contre cette menace (Trojan.Win32.Powemuddy, Trojan.Win32.Seedworm).

- L'organisation caritative « Save the Children » a été victime d'une escroquerie de type « arnaque au président » qui a entraîné le vol de 1 million de dollars. Le pirate a réussi à compromettre le compte de messagerie d'un collaborateur de l'organisation, à se faire passer pour ce collaborateur, et conduire l'organisation à transférer de l'argent à une entité frauduleuse au Japon.

- Une nouvelle campagne de phishing par email associée au groupe russe APT-28 a été détectée, ciblant différents gouvernements et organismes privés, principalement en Ukraine et auprès de membres de l'OTAN.

  La blade Check Point SandBlast offre une protection contre cette menace.

- Une nouvelle variante du logiciel malveillant de suppression de fichiers Shamoon a été découverte, ciblant des entreprises du secteur de l'énergie au Moyen-Orient. Une des cibles est une entreprise italienne de forage pétrolier nommée « Saipem », dont Shamoon a effacé les fichiers sensibles stockés sur environ 10 % de ses serveurs.

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

- Des chercheurs ont découvert que la vulnérabilité zero-day CVE-2018-8611, récemment corrigée dans le noyau Windows, a été exploitée par le groupe SandCat dans le cadre d'attaques contre des entités au Moyen-Orient et en Afrique. Cette vulnérabilité permettrait à des pirates d'exécuter du code arbitraire.

  La blade Check Point IPS offre une protection contre cette menace (Élévation de privilèges dans le noyau Microsoft (CVE-2018-8611)).

VULNÉRABILITÉS ET CORRECTIFS

- Une étude menée par des chercheurs de Check Point a révélé plus de 50 nouvelles vulnérabilités dans un module d'Adobe PDF Reader.

  La blade Check Point IPS offre une protection contre ces menaces (Lecture hors limites dans Adobe Acrobat et Reader (APSB18-09: CVE-2018-4985), lecture hors limites dans Adobe Acrobat et Reader (APSB18-21: CVE-2018-5063), etc.).

- Microsoft a publié ses correctifs mensuels pour le mois de décembre, adressant 39 vulnérabilités, dont neuf critiques et deux zero-day qui ont déjà été exploitée.

  La blade Check point IPS offre une protection contre cette menace (Corruption mémoire du moteur de script Chakra dans Microsoft Edge (CVE-2018-8583), corruption mémoire du moteur de script Chakra dans Microsoft Edge (CVE-2018-8617), etc.).

- Un bug dans l'API de Facebook, qui réside dans son système de partage de photos, a exposé des photos non publiées de 6,8 millions d'utilisateurs à des applications tierces.

- Des chercheurs ont découvert une faille critique surnommée « Magellan » dans le logiciel de gestion de base de données SQLite très populaire. La faille permettrait à des pirates d'exécuter du code arbitraire à distance sur les appareils affectés, provoquer des fuites de mémoire dans les applications, ou empêcher leur fonctionnement.

RAPPORTS ET MENACES

- Un nouveau cheval de Troie Android déguisé en outil d'optimisation de la batterie a dérobé de l'argent auprès d'utilisateurs de PayPal. Le cheval de Troie utilise une nouvelle technique exploitant les fonctions d'accessibilité pour lui permettre d'imiter les clics des utilisateurs, et contourner ainsi les authentifications à deux facteurs de PayPal.

  Les clients de Check Point SandBlast Mobile sont protégés contre cette menace.

- Novidade, un nouveau kit d'exploitation de vulnérabilités, cible les routeurs pour TPE afin de compromettre les appareils qui y sont connectés. Novidade utilise une attaque de « pharming », qui falsifie les requêtes entre sites (CSRF) afin de modifier les paramètres DNS des routeurs et rediriger le trafic des appareils connectés vers une adresse IP contrôlée par les pirates.

  Les blades Check Point IPS et Anti-Virus offrent une protection contre cette menace (Falsification des requêtes entre sites sur TP-LINK WR1043N, kit d'exploitation de vulnérabilités Novidade).

- Un troisième logiciel malveillant MacOS, nommé LamePyre et en cours en développement, a été découvert ce mois-ci. LamePyre se déguise en copie de l'application de messagerie Discord populaire parmi les joueurs. Le logiciel malveillant est capable d'effectuer des captures d'écran et d'ouvrir une porte dérobée pour déclencher d'autres actions. Cette porte dérobée a notamment été détectée dans une autre souche de logiciel malveillant pour macOS, DarthMiner, qui intègre des fonctions d'extraction de crypto-monnaie.

  La blade Check Point Anti-Virus offre une protection contre cette menace (Trojan.OSX.LamePyre).