6-11 novembre 2018

RAPPORT THREAT INTELLIGENCE

PRINCIPALES FAILLES ET ATTAQUES

- Les données personnelles de près de 700 000 clients d'American Express India ont été exposées en ligne en raison d'un serveur MongoDB non sécurisé. Les données exposées comprennent les numéros de téléphone, noms complets, adresses électroniques, champs de description du type de carte, ainsi que les détails des comptes sur americanexpressindia.co.in.

- Plusieurs institutions et ministères italiens ont subi de graves fuites de données et dégradations, imputables à des groupes affiliés à Anonymous en commémoration de la Journée de Guy Fawkes. Parmi les victimes figuraient le Centre national de recherche, l'Institut des technologies de l'éducation et l'Association de la police d'État.

- Un nouveau botnet IRC a été découvert, ciblant principalement les objets connectés et les serveurs Linux, et également des systèmes Android et Windows. Surnommé « Shellbot », le botnet est capable d'effectuer des analyses de ports, des attaques par déni de service distribué et SSH par brute force contre de grandes entreprises.

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

- Des chercheurs ont révélé un nouveau botnet de spam surnommé « BCMPUPnP_Hunter », qui aurait peut-être déjà infecté 400 000 machines. Le botnet cible principalement des routeurs sur lesquels la fonctionnalité UPnP (Universal Plug and Play) de BroadCom est activée, y compris des modèles de routeurs de D-Link, Linksys/Cisco, ZyXEL et autres.

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

- Des pirates ont créé une version .com du site d'information sur les élections « vote411.org » afin de réaliser des escroqueries à l'assistance technique. Ils ont redirigé les visiteurs des plates-formes macOS et iOS vers des pages présentant de fausses alertes d'infection, afin d'amener les victimes à payer pour de faux services d'assistance.

- HSBC Bank USA a été victime d'une fuite majeure de données lorsque des agresseurs non autorisés ont réussi à accéder aux comptes en ligne de l'institution financière. Les données exposées incluent les informations personnelles des clients ainsi que les soldes des comptes, l'historique des transactions, des informations sur les comptes de bénéficiaires, etc.

VULNÉRABILITÉS ET CORRECTIFS

- Des chercheurs de Check Point ont découvert une vulnérabilité critique dans les drones DJI, dans laquelle le même cookie de connexion peut être utilisé pour se connecter à différents utilisateurs DJI. Cette vulnérabilité permettrait à des pirates d'accéder aux différentes plates-formes utilisateur, ainsi qu'à des photos, des vidéos, des carnets et des plans de vol, des flux vidéo en direct, etc.
- Nginx a publié une mise à jour de sécurité pour le logiciel de son serveur web open source, corrigeant plusieurs vulnérabilités de déni de service affectant plus d'un million de serveurs web nginx non corrigés.
- Une vulnérabilité d'exécution de code à distance a été découverte dans le serveur multimédia de streaming open-source Icecast, qui permettrait à des pirates de stopper la diffusion de stations de radio en ligne.
- Une vulnérabilité zero-day dans le logiciel de virtualisation open source populaire VirtualBox a été découverte. Cette vulnérabilité permettrait à un pirate ou à un logiciel malveillant doté de droits root ou administrateur de s'échapper de la machine virtuelle et d'exécuter du code sur le système d'exploitation de la machine hôte.
- Une vulnérabilité zero-day de suppression arbitraire de fichiers a été découverte dans le plugin WordPress populaire WooCommerce. Cette vulnérabilité permettrait à un utilisateur privilégié malveillant ou compromis de réinitialiser le mot de passe d'un compte administrateur et d'obtenir un contrôle total sur des sites web non corrigés.
- Des chercheurs ont découvert plusieurs vulnérabilités critiques dans les lecteurs SSD auto-chiffrés, qui permettraient à un agresseur de déchiffrer les disques et récupérer des données protégées en contournant l'authentification par mot de passe.

RAPPORTS ET MENACES

- Des chercheurs ont découvert le cheval de Troie « FastCash » utilisé par le groupe nord-coréen Lazarus pour mener des attaques frauduleuses contre des guichets automatiques. Les pirates compromettent les serveurs d'application gérant les transactions des guichets automatiques à l'aide d'identifiants dérobés sur les réseaux des banques, pour traiter les demandes de retraits.

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

- Des chercheurs ont découvert une nouvelle campagne Emotet utilisant des macros malveillants intégrées à des pièces jointes aux formats Word et PDF. La nouvelle campagne contient de nouveaux modules d'attaque améliorés, notamment un module d'exfiltration conçu pour collecter les emails des ordinateurs infectés.

  Les blades Check Point Anti-Bot et Anti-Virus offrent une protection contre cette menace (Trojan.Win32.Emotet).

- Une nouvelle variante d'un logiciel malveillant d'extraction de cryptomonnaie a été découverte, ciblant Linux et capable de masquer la présence de son processus malveillant aux outils de surveillance à l'aide d'un rootkit. Les systèmes infectés peuvent uniquement témoigner d'une utilisation élevée du processeur, sans pouvoir détecter le processus source qui en est la cause.