26 novembre – 2 décembre 2018

RAPPORT THREAT INTELLIGENCE

PRINCIPALES FAILLES ET ATTAQUES

- Des chercheurs de Check Point ont révélé un nouvel extracteur de Monero appelé « KingMiner », ciblant des serveurs Windows IIS et SQL lors d'attaques par brute force. KingMiner est configuré pour utiliser 75 % des ressources du processeur, et il utilise différentes techniques d'évasion pour contourner les méthodes d'émulation et de détection.

  Les blades Check Point IPS, Anti-Bot et Anti-Virus offrent une protection contre cette menace (Téléchargeur de script suspect, XML contenant des fichiers malveillants, Trojan.Win32.KingMiner).

- Marriott international a été victime d'une fuite de données majeure qui a compromis 500 millions de dossiers clients. Les pirates ont eu accès à la base de données de réservations de sa filiale « Starwood Hotels », qui contient les informations personnelles et les détails des réservations des clients, ainsi que leurs numéros de carte bancaire.

- Un pirate a réussi à dérober 1 million de dollars auprès d'un cadre de la Silicon Valley via une escroquerie par échange de carte SIM. Le pirate a usurpé l'identité de la victime pour réaffecter son numéro de téléphone à une carte SIM appartenant au pirate, et il a réussi à dérober l'argent des comptes de la victime sur Coinbase et Gemini.

- Une attaque de logiciel rançonneur a frappé les systèmes informatiques de l'l'hôpital régional de l'état de l'Ohio et a perturbé ses salles d'urgence, obligeant l'hôpital à acheminer ses patients vers d'autres salles d'urgence. À la fin de la semaine, les systèmes du nouveau téléphérique de Moscou ont également été visés par une attaque de logiciel rançonneur.

- Un pirate a réussi à détourner 50 000 imprimantes connectées à Internet dans le monde entier afin d'imprimer des flyers invitant les utilisateurs à s'abonner à la chaîne YouTube de « PewDiePie ». Le pirate a trouvé des imprimantes vulnérables à l'aide de Shodan et a utilisé un kit d'exploitation de vulnérabilités d'imprimantes pour lancer des commandes sur les imprimantes non protégées.

- Dunkin' Donuts a été victime d'une fuite de données exposant les informations personnelles des clients, notamment leurs noms, adresses électroniques et détails de leur compte associé au programme de fidélité. Le pirate a utilisé une technique de « credential stuffing », injectant des identifiants obtenus à partir de failles de sécurité antérieures.

- Huit applications Android populaires exploitées par « Cheetah Mobile » et « Kika Tech » ont été impliquées dans une escroquerie à la publicité. Les sociétés sont accusées d'avoir abusé des permissions des applications pour surveiller les téléchargements de nouvelles applications, et d'avoir manipulé les données des utilisateurs pour récupérer frauduleusement les sommes versées pour leur installation.

VULNÉRABILITÉS ET CORRECTIFS

- Une vulnérabilité critique d'exécution de commande non autorisée a été découverte dans l'application de conférence de la société Zoom. Cette vulnérabilité permettrait à un pirate distant de prendre le contrôle des écrans, d'usurper les messages de discussion, d'expulser des participants et les empêcher de se reconnecter aux conférences.

  La blade Check Point IPS offre une protection contre cette menace (Contournement de la restriction de sécurité de répertoire FilesMatch dans Apache httpd).

- Du code malveillant visant à dérober les fonds stockés dans des applications de portefeuille Bitcoin a été injecté dans un module tiers NodeJS téléchargé 2 millions de fois par semaine. Le code malveillant a été injecté par le développeur gérant le module, après qu'il ait pris la place du développeur d'origine pour se charger de la maintenance du script.

- Cisco a publié un correctif de sécurité adressant une faille critique dans deux de ses outils de gestion de licences. La faille permettrait à un pirate distant non authentifié d'exécuter des requêtes SQL arbitraires, et modifier et supprimer des données aléatoires dans les applications de gestion du cycle de vie des produits Cisco.

- Cisco a réédité un correctif de sécurité pour une grave vulnérabilité d'élévation de privilèges dans sa plate-forme WebEx Meetings, après que des chercheurs aient réussi à contourner le premier correctif. La faille réside dans le service de mise à jour de l'application et permettrait à un pirate local d'élever ses privilèges.

  La blade Check Point IPS offre une protection contre cette menace (Injection de commandes dans le service de mise à jour de l'application Cisco Webex Meetings).

RAPPORTS ET MENACES

- Des chercheurs de Check Point ont publié un rapport détaillé sur l'évolution du cheval de Troie bancaire « BackSwap » nouvellement découvert, et ses techniques malveillantes améliorées. Le rapport a révélé que BackSwap a transformé ses activités malveillantes pour se focaliser presque entièrement sur des banques espagnoles.

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

- Le logiciel espion mobile « Rotexy » s'est transformé en cheval de Troie sophistiqué comportant des techniques d'évasion et des fonctionnalités à la fois de logiciel malveillant bancaire et de logiciel rançonneur. Rotexy se propage par SMS de phishing, et a déjà déclenché 70 000 attaques contre des utilisateurs principalement basés en Russie.

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

- Des chercheurs ont développé des applications mobiles utilisant des fonctionnalités des ampoules intelligentes pour exfiltrer des données. La première application est installée sur l'appareil mobile de la victime et l'autre sur l'appareil mobile du pirate pour recevoir et intercepter les données, en utilisant la lumière comme moyen de transfert des données volées.

- Des chercheurs ont découvert un nouvel extracteur de cryptomonnaie puissant et modulaire sur Linux. La structure de l'extracteur de cryptomonnaie possède plusieurs composants qui implémentent une vaste gamme de fonctionnalités, notamment l'arrêt des processus d'autres extracteurs, la suppression des logiciels antivirus, le téléchargement de logiciels malveillants supplémentaires et le lancement d'attaques DDoS.