Check Point
SOFTWARE TECHNOLOGIES LTD.

2 - 8 janvier 2017

RAPPORT THREAT INTELLIGENCE

PRINCIPALES FAILLES ET ATTAQUES

- Plus de 10 000 bases de données MongoDB vulnérables, soit 25 % des serveurs Internet accessibles de ce type, ont été frappés par des logiciels rançonneurs au cours des semaines précédentes. Plusieurs groupes de pirates tentent d'exploiter une vulnérabilité récemment découverte. Ils dérobent les données de ces bases et les restituent à leurs propriétaires pour 0,2 bitcoin de rançon.
- Les informations personnelles de millions d'Israéliens risquent d'être publiées, suite à la découverte de graves failles de sécurité dans l'application Waterly, qui est utilisée pour payer les factures d'eau. Selon des chercheurs, l'application ne vérifie pas qu'un utilisateur est bien relié à un compte spécifique, ce qui permet aux pirates d'accéder aux informations de facturation de chaque utilisateur enregistré.
- Une escroquerie de « support technique » ciblant les utilisateurs de Mac a été découverte. Après avoir consulté une URL malveillante, les utilisateurs sont touchés par l'une des deux exploitations de vulnérabilité possibles, qui provoque un déni de service par l'ouverture de nouveaux emails ou de fichiers audio jusqu'à ce que la machine cesse de fonctionner. Les utilisateurs sont ensuite amenés à contacter un faux numéro de support technique et régler une somme aux agresseurs.
- Une base de données contenant des renseignements personnels sur des militaires américains a été découverte par des chercheurs en sécurité après avoir été accidentellement publiée par un prestataire. On ne sait pas si cette base a été consultée par d'autres personnes et l'on ne connaît pas le nombre de personnes dont les renseignements ont été divulgués.
- Le groupe de piratage DragonOK, associé à la Chine, a récemment lancé des attaques sur des cibles à Taiwan, en Russie et au Japon. Le groupe a utilisé des emails de phishing et une vulnérabilité dans Microsoft Office via des fichiers RTF malveillants.

La blade Check Point IPS offre une protection contre ces menaces (Corruption mémoire dans Microsoft Office (MS15-033: CVE-2015-1641)).

VULNÉRABILITÉS ET CORRECTIFS

- Google a publié une mise à jour de sécurité pour Android, contenant des correctifs pour plus de 90 failles de sécurité dans plusieurs composants.
- Une vulnérabilité dans le système d'inspection du trafic HTTPS de Kaspersky a été découverte. Elle permettrait à des agresseurs d'accéder à des certificats SSL racine sur des machines protégées par Kaspersky. Kaspersky a depuis corrigé cette vulnérabilité.
- La fonctionnalité de pré-remplissage de formulaires disponible dans plusieurs navigateurs Internet pourrait être un vecteur de phishing potentiel pour les agresseurs. Selon une étude, une page de connexion pourrait contenir des champs cachés qui peuvent être automatiquement remplis par le navigateur, en plus des champs présentés à l'utilisateur.

RAPPORTS ET MENACES

- Check Point a publié une analyse du logiciel rançonneur Goldeneye, la nouvelle variante du logiciel rançonneur Petya. Goldenye a lancé une campagne d'emails ciblant les départements de RH d'entreprises, en particulier en Allemagne, puisqu'ils doivent ouvrir des documents provenant de sources inconnues dans le cadre de leur travail quotidien.

  Les blades Check Point IPS et SandBlast Zero Day Protection offrent une protection contre cette menace (Fichiers Microsoft Office contenant du code VBScript malveillant de téléchargement).

- Une analyse détaillant le processus technique de la vulnérabilité d'exécution de code à distance PHPMailer a été publiée.

  La blade Check Point IPS offre une protection contre cette menace (Exécution de code à distance sur PHPMailer Mail From).

- Check Point a publié une analyse du logiciel malveillant utilisé dans des attaques contre le principal système de messagerie financière SWIFT, qui ont entraîné la perte de millions de dollars. Selon l'analyse, le logiciel malveillant a été spécialement conçu grâce à des connaissances des processus de travail et du système SWIFT.
- Le logiciel malveillant Switcher infecte des téléphones mobiles en se faisant passer pour une application légitime. Il tente alors une attaque par brute force contre les routeurs auxquels les téléphones sont connectés, à l'aide des mots de passe par défaut connus, afin de détourner le DNS et rediriger le trafic vers des sites web malveillants.