OUCH! | Juin 2017

La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

OUCH!

Dans ce numéro...

Leçons à tirer du ransomware WannaCry

Vue d'ensemble

Récemment, vous avez probablement vu en une des journaux une information relative à une nouvelle attaque cybernétique appelée "WannaCry". "WannaCry" a infecté plus de 200 000 ordinateurs, bloquant les données d'une variété d'organisations y compris celles des hôpitaux au Royaume-Uni. Il y'a plusieurs raisons pour lesquelles cette attaque a suscité tant d'attention. Tout d'abord, elle se répand rapidement d'un ordinateur à un autre en attaquant une faiblesse connue dans les ordinateurs Windows. Deuxièmement, l'attaque était un type de malware appelé "ransomware", ce qui signifie qu'une fois qu'il a infecté votre ordinateur, il chiffre tous vos fichiers, verrouillant ainsi vos données. La seule façon de récupérer vos données est d'avoir effectué des sauvegardes au préalable ou de payer à l'attaquant une rançon de 300 $ pour décrypter toutes vos données. Troisièmement, et surtout, cette attaque n'aurait jamais dû être en mesure de se produire. La faiblesse "WannaCry" qui attaquait les ordinateurs Windows était bien connue de Microsoft qui avait publié un correctif des mois plus tôt. Mais de nombreuses organisations n'ont pas installé la solution, ou utilisent toujours des systèmes d'exploitation comme Windows XP, trop vieux. Du coup, les correctifs ne sont plus disponibles. Voici trois étapes simples que vous pouvez prendre en considération pour vous assurer que les attaques comme "WannaCry" ne vous infectent jamais.

Editeur invité

Dr. Johannes Ullrich est le doyen de la recherche du SANS Technology Institute et le fondateur de DShield.org. Il est responsable du **SANS Internet Storm Center** qui surveille les menaces actuelles de sécurité informatique. Il enseigne les cours Web Application Security (**DEV522**), Intrusion Detection (**SEC503**) et IPv6 (**SEC546**).

Correctifs

D'abord et avant tout, assurez-vous que vos ordinateurs, appareils mobiles, applications et tout ce qui est connecté à Internet soient à jour. Les cybercriminels recherchent constamment de nouvelles vulnérabilités dans le logiciel utilisé par vos appareils. Lorsqu'ils découvrent des vulnérabilités, ils utilisent des programmes spéciaux pour pirater les appareils que vous utilisez. Pendant ce temps, les entreprises qui ont créé le logiciel pour vos appareils travaillent dur pour résoudre ces vulnérabilités en publiant les mises à jour et en veillant à ce que vos ordinateurs et appareils mobiles installent ces mises à jour. Ainsi, il est beaucoup plus difficile pour quelqu'un de vous pirater. C'est ce qui est si frustrant avec la propagation de WannaCry. Les mises à jour pour réparer et arrêter cette attaque ont été publiées presque deux mois plus tôt par Microsoft. Si les organisations avaient gardé leurs ordinateurs à jour, cette attaque n'aurait jamais fonctionné. Pour vous assurer

Leçons à tirer du ransomware WannaCry

que vos appareils restent à jour, activez la mise à jour automatique autant que possible. Cette règle s'applique à presque toutes les technologies connectées à un réseau, pas seulement vos ordinateurs et appareils mobiles, mais des téléviseurs connectés à Internet, des routeurs maison, des consoles de jeux ou un jour, peut-être même votre voiture. Si vos systèmes d'exploitation ou vos périphériques sont si anciens qu'ils ne sont plus pris en charge par des mises à jour de sécurité, tels que Windows XP, il faut les remplacer par des plus récents.

La clé pour vous protéger des attaques comme WannaCry est en trois étapes simples. Gardez vos ordinateurs mis à jour, soyez vigilants aux attaques de phishing et sauvegardez vos systèmes.

Sauvegardes

Dans certains cas, les cyberattaques comme le ransomware peuvent même infecter des systèmes à jour. Voici une deuxième façon de vous protéger et de sauvegarder vos données. Les sauvegardes sont des copies de vos informations stockées ailleurs que sur votre ordinateur ou votre appareil mobile. Lorsque vous perdez des données précieuses, vous pouvez récupérer ces données à partir de vos sauvegardes. Malheureusement, trop de personnes ne parviennent pas à effectuer des sauvegardes régulières, même si elles sont simples et peu coûteuses. Il existe deux façons de sauvegarder vos données : les médias physiques ou le stockage basé sur le cloud. Chaque approche présente des avantages et des inconvénients. Vous pouvez utiliser les deux approches en même temps si vous ne savez pas quelle méthode utiliser.

Les médias physiques sont des appareils que vous contrôlez, tels que les lecteurs USB externes ou les lecteurs connectés au réseau situé dans votre maison ou votre bureau. L'avantage d'utiliser vos propres médias physiques est qu'ils vous permettent de sauvegarder et de récupérer de nombreuses quantités de données très rapidement. L'inconvénient d'une telle approche est que si vous êtes infecté par des logiciels malveillants, tels que le ransomware, il est possible que l'infection se propage à vos sauvegardes. Si vous utilisez des supports physiques pour les sauvegardes, vous devez stocker des copies de votre sauvegarde hors site dans un emplacement sécurisé. Assurez-vous que les sauvegardes que vous stockez sont correctement étiquetées. Les solutions basées sur le cloud sont des services en ligne qui sauvegardent et stockent vos fichiers sur Internet. En règle générale, vous installez un programme sur votre ordinateur qui prend tout en charge. Les avantages des solutions sur le cloud sont leur simplicité. En outre, si vous êtes infecté par un ransomware, l'infection ne peut généralement pas accéder à vos sauvegardes basées sur le cloud. Les inconvénients sont que cela peut prendre beaucoup de temps pour sauvegarder ou récupérer de très grandes quantités de données. Assurez-vous de

Leçons à tirer du ransomware WannaCry

rechercher la confidentialité et la sécurité des sauvegardes du cloud. Le service de sauvegarde offre-t-il une sécurité forte, comme le cryptage de vos données et l'authentification forte ?

Hameçonnage

Enfin, les cybercriminels sont toujours en train de mettre à jour et de changer leurs méthodes d'attaque. Ils utilisent souvent une autre méthode d'attaque appelée hameçonnage pour attaquer et infecter leurs victimes. les cybercriminels vous envoient un courrier électronique tentant de vous inciter à ouvrir une pièce jointe infectée ou à visiter un site Web malveillant. Si vous le faites, votre ordinateur risque d'être infecté. Alors que "WannaCry" n'a pas utilisé cette méthode d'attaque, elle est couramment utilisé pour de nombreux autres types d'attaques, y compris la plupart des types de ransomware. En outre, les cybercriminels qui ont développé WannaCry mettront sans aucun doute à jour leurs méthodes d'attaque dans les mois à venir et utiliseront de nouvelles techniques telles que le phishing pour infecter encore plus d'ordinateurs. La clé pour vous protéger contre ces attaques par courrier électronique est votre bon sens. Si un courrier électronique ou un message semble étrange, suspect ou trop bon pour être vrai, il est très probable qu'il s'agisse d'une attaque.

Version Française

La division sécurité de ANSWER S.A. offre des services de Conseil, d'Audit et d'Architecture en sécurité des systèmes d'information. Ces activités sont accompagnées d'une veille active sur les solutions de sécurité du marché permettant ainsi à ses consultants de répondre efficacement aux problématiques de ses clients. Pour en savoir plus, veuillez vous référer aux liens suivants : http://www.answer.ch et http://answersecurity.com/

Sources

Qu'est-ce qu'un Malware :	https://securingthehuman.sans.org/ouch/2016#march2016
Ransomware :	https://securingthehuman.sans.org/ouch/2016#august2016
Sauvegardes :	https://securingthehuman.sans.org/ouch/2015#august2015
Hameçonnage :	https://securingthehuman.sans.org/ouch/2015#december2015
Utiliser le cloud en toute sécurité :	https://securingthehuman.sans.org/ouch/2016#november2016

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traduit par : Marilyn Combet