Communiqué de presse

Contact Presse :
Annabelle Sou
Fortinet, Inc.
04 89 87 05 76
asou@fortinet.com

Le Rapport de Fortinet sur les Principales Menaces du mois de Novembre Souligne une Réduction des Niveaux de Spams après le Retrait de Bredolab

Les Serveurs Koobface ont démontré le 14 Novembre qu'ils ont pu être Reconfigurés à de Nouveaux Serveurs de Contrôle 5 Jours Plus Tard

Sophia Antipolis, 3 Décembre 2010 - Fortinet® (NASDAQ: FTNT) l'un des principaux acteurs du marché de la sécurité réseau et le leader mondial des systèmes unifiés de sécurité UTM (Unified Threat Management) – publie aujourd'hui son rapport sur les principales menaces du mois de Novembre 2010, qui met en évidence une réduction de 12% de spams dans le monde après que les autorités Néerlandaises aient démantelé un vaste réseau nommé Bredolab. De ce fait, elles ont pris possession de plus de 140 serveurs hors connexion.

"*Bredolab a souvent été utilisé pour charger des moteurs de spams, qui sont généralement destinés à vendre des produits pharmaceutiques contrefaits*," déclare Derek Manky, chef de projet en cybersécurité et recherche des menaces chez Fortinet. "*L'ampleur de Bredolab a eu un impact énorme sur le niveau de spams, chutant de 26% en une semaine après avoir été démantelé*."

Le retrait de Koobface

Koobface, un botnet bien connu pour se propager sur les sites de réseaux sociaux populaires, a été rendu inopérant le 14 Novembre lorsque Coreix, un FAI anglais a déconnecté 3 serveurs MotherShip. Koobface utilisait des serveurs intermédaires (proxys) pour communiquer avec ces serveurs MotherShip via le port 80.

"*Nous confirmons que le 14 Novembre, lorsque les serveurs de base sont passés en hors connexion, les serveurs intermédiaires n'ont plus rien relayés, ce qui a effectivement paralysé le botnet*," poursuit Derek Manky . "*Malheureusement, nous avons vu la communication restaurée 5 jours plus tard, le 19 Novembre. Cela est probablement dû au fait que Koobface contient un module de vol de mots de passe FTP*."

Les opérateurs peuvent utiliser les informations d'identification FTP volées pour transformer des serveurs Web en proxys. En pointant leurs serveurs intermédiaires vers les nouveaux serveurs MotherShip, les opérateurs semblent reprendre le contrôle de leur botnet.

Les vulnérabilités Zero-day d'Adobe, Microsoft, Apple

En Novembre, FortiGuard labs a également révélé des vulnérabilités zero-day dans Adobe Shockwave (FGA-2010-54), Adobe Flash (FGA-2010-56), Microsoft Office PowerPoint (FGA-2010-58), et Apple QuickTime (FGA-2010-61). En plus des 4 zero days, 146 nouvelles vulnérabilités supplémentaires ont été découvertes par FortiGuard IPS; 40% d'entres elles ont été activement exploitées. A ce jour, une vulnérabilité zero-day est encore exploitée pour Microsoft Internet Explorer (FGA-2010-55). Les 5 vulnérabilités ont été décisives, et avaient le potentiel de permettre aux attaquants d'exécuter un code arbitraire à distance.

Les nouvelles et anciennes vulnérabilités continueront à être exploitées, il est donc important de garder toutes les applications mises à jour. En outre, un système de prévention d'intrusions valide (IPS) peut aider à atténuer les attaques contre l'ensemble des vulnérabilités connues et zero-days. Grâce à l'utilisation de la communication par des protocoles communs, le contrôle des applications est devenu de plus en plus important pour identifier l'activité malicieuse au niveau des applications.

FortiGuard Labs a compilé des statistiques et tendances de menaces pour Novembre à partir de données recueillies par les appliances de sécurité réseau FortiGate® et des systèmes

d'intelligence. Les clients qui utilisent les FortiGuard Services de Fortinet devraient être protégés contre ces vulnérabilités.

Les FortiGuard Services offrent des solutions de sécurité de grande envergure dont un antivirus, la prévention d'intrusions, le filtrage du contenu Web et un anti-spam. Ces services assurent une protection contre les menaces sur l'ensemble des couches applicatives et du réseau. Les FortiGuard Services sont mis à jour par le FortiGuard Labs, qui permet à Fortinet d'offrir une sécurité multi-couches et une protection rapide contre les menaces nouvelles et émergentes. Pour les clients abonnés à FortiGuard, ces mises à jour sont livrées sur tous les produits FortiGate®, FortiMail™ et FortiClient™.

La version intégrale du Threat Landscape report de Novembre, comprenant le classement des menaces les plus élevées dans plusieurs catégories, est d'ores et déjà disponible. Les recherches en cours sont consultables au FortiGuard Center ou via FortiGuard Labs' RSS feed. D'autres discussions sur les technologies de sécurité et les analyses des menaces sont disponibles sur Fortinet Security Blog.

A propos de Fortinet (www.fortinet.com)

Fortinet (code NASDAQ : FTNT) est un des principaux fournisseurs de solutions de sécurité réseau et le leader du marché des systèmes unifiés de sécurité *Unified Threat Management* ou UTM. Nos produits et services d'abonnements assurent une protection étendue, intégrée et efficace contre les menaces dynamiques, tout en simplifiant l'infrastructure de sécurité informatique. Parmi nos clients figurent des administrations, des fournisseurs d'accès et de nombreuses entreprises, dont la plupart font partie du classement 2009 du Fortune Global 100. FortiGate, le produit phare de Fortinet, intègre des processeurs ASIC pour une meilleure performance et plusieurs fonctions de sécurité conçues pour protéger les applications et les réseaux contre les menaces Internet. Au-delà de ses solutions UTM, Fortinet offre une large gamme de produits conçus pour protéger le périmètre étendu des entreprises – du terminal au périmètre et au cœur de réseau, en passant par les bases de données et applications. Fortinet, dont le siège social se trouve à Sunnyvale en Californie (États-Unis), dispose également de bureaux dans le monde entier.

###

FortiWeb. L'ensemble des marques commerciales citées dans le présent communiqué sont la propriété de leurs détenteurs respectifs. Fortinet n'a pas vérifié de façon indépendante les déclarations ou les certificats ci-dessus attribuées à des tiers et Fortinet n'a pas approuvé de telles déclarations. Le présent communiqué peut contenir des déclarations prévisionnelles impliquant des incertitudes et des hypothèses. Si les risques ou les incertitudes se concrétisent ou si les hypothèses se révèlent inexactes, les résultats peuvent différer sensiblement par rapport à ceux exprimés ou sous-entendus. Toutes les déclarations autres que celles des faits historiques sont des déclarations qui pourraient être considérées comme des déclarations prévisionnelles, dont mais sans s'y limiter des déclarations liées aux tendances de l'activité des cybercriminels. Ces tendances sont difficiles à prédire et les prévisions exprimées au sujet de ces tendances peuvent au final ne pas être correctes. Fortinet n'a aucune obligation de mettre à jour les déclarations prévisionnelles dans l'éventualité où les résultats réels diffèrent et n'en a pas l'intention.

FTNT-O