Image not found or type unknown

Cybercriminalité : Etat des lieux

Conseils pratiques publié le **31/10/2016**, vu **900 fois**, Auteur : Legicia Détective Privé

41,8 % des divulgations de vulnérabilités sont évaluées comme très graves. C'est le pourcentage le plus élevé depuis trois ans.

Les divulgations de vulnérabilités sont des révélations de failles logicielles au grand public. Leurs sources sont variées : éditeurs des logiciels concernés, fournisseurs de logiciels de sécurité, chercheurs indépendants dans le domaine de la sécurité, voire les créateurs mêmes des programmes malveillants.

Les pirates et les programmes malveillants tentent généralement d'utiliser des failles non protégées en vue de mettre en danger et de s'en prendre aux organisations.

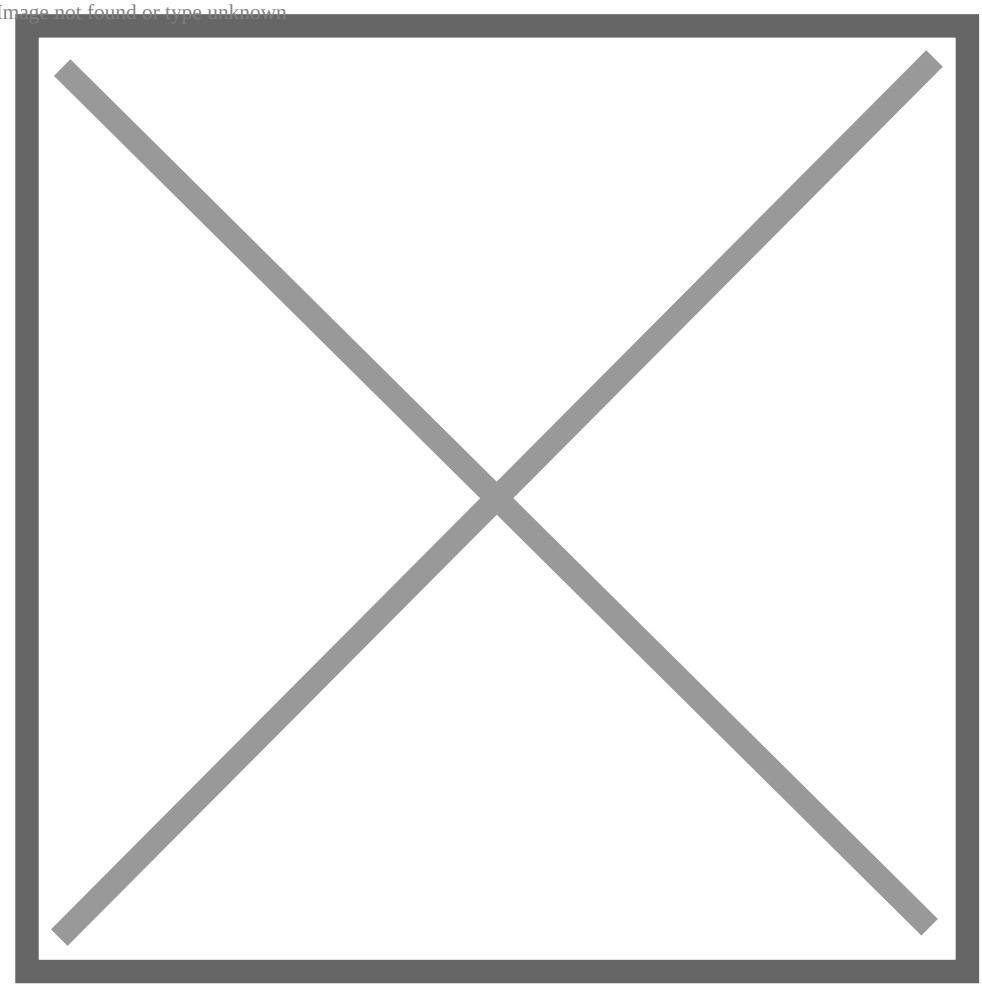
Dans le secteur, les divulgations de vulnérabilités ont augmenté de 9,4 % entre les premier et le second semestres de 2015, pour dépasser de peu les 3 300. Il s'agit des vulnérabilités très graves que redoutent les équipes en charge de la sécurité dans la mesure où elles risquent d'impliquer des pirates distants.

Avec plus de 6 000 vulnérabilités divulguées au public tous les ans dans le secteur, il est absolument crucial de veiller à l'évaluation et à la mise à jour régulières de l'ensemble des logiciels que compte votre environnement IT. Installez les correctifs logiciels sans tarder, détectez toute activité suspecte sur les réseaux et placez en quarantaine les appareils au comportement anormal.

Les pays enregistrant le plus fort taux d'infection de logiciels malveillants sont la Mongolie, la Libye, les Territoires palestiniens, l'Irak et le Pakistan.

Taux d'infection par pays/région

Image not found or type unknown



Les attaques de type cheval de Troie, une catégorie de programmes malveillants prédominante qui s'appuie sur le piratage psychologique pour abuser les utilisateurs, a augmenté de 57 % et se maintient à des niveaux élevés.

Les chevaux de Troie prétendent être quelque chose qui ressemble à un document ou à une vidéo. Il s'agit en réalité d'un outil qu'utilisent les pirates pour tromper les gens en leur faisant réaliser des actions qui vont à l'encontre de leurs intérêts, comme l'installation de logiciels malveillants sur leur système ou l'affaiblissement de leurs paramètres de sécurité. C'est pourquoi les chevaux de Troie figurent parmi les outils favoris des pirates. Sachant cela et en observant comment se comportent les chevaux de Troie les plus nuisibles dans votre région, vous serez mieux armé pour protéger votre organisation.
Formez votre personnel aux ruses des chevaux de Troie, y compris sur les articles web factices aux titres provocateurs et sur les adresses e-mail usurpées. Encouragez les employés à utiliser leurs propres appareils au lieu des appareils connectés au réseau de votre entreprise pour surfer sur le web et utiliser les médias sociaux.

De nombreuses type d'attaques existent :

hameçonnage (phishing)

Rançongiciel» (ransomware)

Vous pouvez également signaler les faits dont vous avez été victime via la plateforme de signalement « Pharos » ou le numéro dédié : 0811 02 02 17
Des services spécialisés se chargent ensuite de l'enquête :

- Police nationale : l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) qui dépend de la Sous-direction de lutte contre la cybercriminalité (SDLC) : 01 47 44 97 55
- Gendarmerie nationale : le centre de lutte contre les criminalités numériques (C3N) du Service Central du Renseignement Criminel (SCRC) : cyber@gendarmerie.interieur.gouv.fr
- Préfecture de police : la Préfecture de police de Paris, de la Direction centrale du renseignement intérieur (DCRI) et ses équipes de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) compétente uniquement pour Paris et petite couronne (75, 92, 93 et 94) : 01 40 79 67 50

Pour plus d'informations, rendez-vous sur le site du Ministère de l'Intérieur, en charge de la lutte contre la cybercriminalité.