

ACTU NEWS ANTIVIRUS, ANTISPAM, CYBER CRIMINALITÉS

Niveaux de Risque d'Epidémies Virales

Kaspersky Lab utilise trois niveaux de menaces: vert, signifiant que l'activité virale est normale ; orange, signifiant que le risque d'infection est plus élevé qu'à la normale ; et rouge signifiant que le danger d'infection est très élevé. Vert : l'activité virale est normale

L'activité virale est continue. Ce niveau signifie qu'il n'y a pas de nouvelles menaces à l'horizon et que les ordinateurs pourvus de bases antivirus mises à jour et de patches récents sont en sécurité.



Vert : alerte informationnelle



Une alerte à titre d'information sera donnée:

Si l'envoi en masse d'un programme malicieux est détecté. Même si le programme en lui-même ne représente pas un grand danger, le mailing de masse peut mener à une sérieuse épidémie à cause du très grand nombre d'infections.

Si les analystes de Kaspersky Lab reçoivent un échantillon d'un programme malicieux doté d'une fonctionnalité unique, ou un code de proof-of-concept, ou un programme qui n'est pas une menace directe mais possède un intérêt technique.



Orange: alerte moyenne



Ce niveau signifie qu'un programme malicieux spécifique peut représenter un danger même pour les machines équipées de patchs mis à jour et de protection antivirus. L'alerte orange sera donnée si:

Plus de 10 messages de détection ou d'infection par le programme malicieux sont envoyés par des internautes en l'espace de 4 heures

Si le programme malicieux est une nouvelle modification d'un programme ayant par le passé causé une sérieuse épidémie

Si le programme malicieux use d'une vulnérabilité critique ou de vulnérabilités dans Windows pour se propager



Rouge: alerte rouge



Ce niveau est le plus élevé et signifie qu'un programme malicieux se propage rapidement, représentant un véritable danger pour la majorité des systèmes. L'alerte rouge est donnée lorsque :

Un grand nombre d'infections (plusieurs centaines) sont détectées dans les 24 heures. Cela inclut aussi bien des échantillons qui arrivent indépendamment à Kaspersky Lab ou qui sont détectés chez des partenaires

Le programme malicieux est fortement présent dans le trafic Internet. Cette information provient des analystes de Kaspersky Lab et d'autres organisations majeures de recherche tels que MessageLabs, CERT et SANS

L'épidémie peut conduire à une perte de connexion (à court ou long terme, partielle ou totale) dans les segments Internet

La décision de publier une alerte est prise par les analystes viraux de Kaspersky Lab, qui traquent les logiciels malveillants 24h/24.

<http://www.viruslist.com/fr/viruses/alerts?chapter=161596873>

Commentaires

2010-11-03 15:05:34 - og

En ce qui me concerne j'ai rapidement survolé les différents modules et n'ai pas encore eu le temps de prendre connaissance du fond de manière plus approfondie, mais je suis persuadée, que ce travail, qui m'apparaît d'ores et déjà très sérieux saura sans aucun doute nous être très utile !!

Copyright : sergey - 2009-09-12 17:22:26
Creative Commons Deed

Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.5

Vous êtes libres :

- * de reproduire, distribuer et communiquer cette création au public

Selon les conditions suivantes :

Paternité. Vous devez citer le nom de l'auteur original.

Pas d'Utilisation Commerciale. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.

Pas de Modification. Vous n'avez pas le droit de modifier, de transformer ou d'adapter cette création.

* A chaque réutilisation ou distribution, vous devez faire apparaître clairement aux autres les conditions contractuelles de mise à disposition de cette création.

* Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits.

Ce qui précède n'affecte en rien vos droits en tant qu'utilisateur (exceptions au droit d'auteur : copies réservées à l'usage privé du copiste, courtes citations, parodie...)

Ceci est le Résumé Explicatif du Code Juridique (la version intégrale du contrat).

<http://creativecommons.org/licenses/by-nc-nd/2.5/>