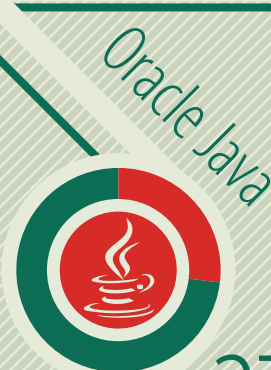


# LOGICIELS VULNÉRABLES

L'une des plus dangereuses menaces pour les entreprises

TOP 3

Programmes les plus fréquemment exploités :



## NOMBRE TOTAL de vulnérabilités identifiées :

2011

4 151

1 822

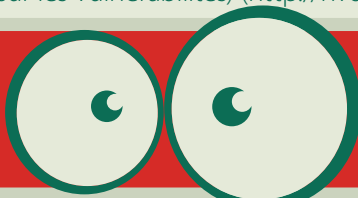
2012

3 782

1 290

RISQUE ÉLEVÉ

Source : National Institute of Standards and Technology, National Vulnerabilities Database (Base de données nationale sur les vulnérabilités) (<http://nvd.nist.gov>) en septembre 2012



## POURQUOI SONT-ILS DANGEREUX ?

### PROPAGATION DE MALWARE



L'ouverture d'un site Web ou d'un document PDF malveillant suffit pour infecter l'ordinateur d'un employé  
Une clé USB infectée est un autre vecteur courant d'attaque

L'infection peut ensuite se répandre dans l'ensemble de l'infrastructure

Les cybercriminels sont ensuite libres de voler les données qu'ils veulent

### ATTAQUES CIBLÉES

1 Un e-mail est envoyé à un employé en particulier

2 Il comporte une pièce jointe malveillante

3 L'ouverture de cette pièce jointe infecte le PC

4 Les cybercriminels prennent ensuite le contrôle total du système de l'utilisateur

5 Et volent des données ou effectuent des transferts depuis les comptes de l'entreprise

## QUATRE ÉTAPES POUR PROTÉGER VOTRE ENTREPRISE

1

Sachez quels logiciels sont installés sur tous vos terminaux :

Limitez l'utilisation des programmes inutiles  
Contrôlez l'activité en ligne de vos employés

2

Obtenez des informations précises sur les logiciels potentiellement vulnérables :

Effectuez une analyse centralisée des vulnérabilités

3

Mettez régulièrement à jour votre système et tous les logiciels installés :

La gestion des correctifs (Patch Management) vous aide à automatiser cette tâche

4

Déployez une technologie fiable de protection contre les programmes malveillants :

Kaspersky Endpoint Security est capable de détecter les menaces, même les nouvelles ou les inconnues, en utilisant une analyse heuristique, Kaspersky Security Network et la technologie System Watcher