

# Bilan de l'année virale 2008

Par Pierre Marc Bureau, Chercheur en malware chez ESET



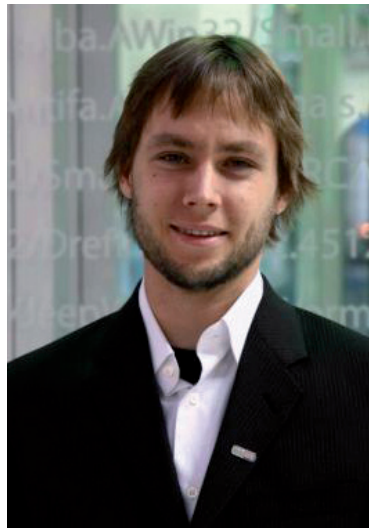
we protect your digital worlds

## Quels nouveaux types de malware ont retenu votre attention en 2008 ?

L'année 2008 a été riche en rebondissements en ce qui concerne les logiciels malveillants. Les faux antivirus ont particulièrement retenu notre attention cette année. Ces logiciels d'extorsion envoient des messages d'alerte aux utilisateurs, indiquant que leur ordinateur est infecté par une multitude de menaces inconnues. Pour se débarrasser des fausses menaces, la victime doit payer quelques dizaines d'euros. Après paiement, le faux antivirus se désactive.

Les tentatives d'extorsions ne sont pas nouvelles sur Internet mais la sophistication et l'envergure de ce type d'attaque sont sans précédent.

Quoique ces menaces demeurent marginales, ESET a découvert de nouveaux échantillons de logiciels malveillants s'attaquant aux téléphones portables. Considérant que ces équipements électroniques sont de plus en plus puissants et utilisés quotidiennement pour surfer sur Internet et consulter des courriers électroniques, il n'est pas surprenant qu'ils soient la cible d'acteurs malveillants.



Pierre-Marc Bureau  
Chercheur en malware  
chez ESET



## Quels sont les nouveaux modes de propagation des menaces ?

En 2008, nous avons eu à traiter un grand nombre de nouvelles menaces utilisant des modes de propagation novateurs. Plusieurs types de fichiers différents ont été utilisés pour lancer des attaques. Nous avons recensé par exemple des dizaines de milliers de fichiers PDF «malveillants» utilisés pour installer des malware sur les ordinateurs «victimes».

Plusieurs failles dans les lecteurs de contenu Flash ont aussi été exploitées pour infecter les ordinateurs visitant des sites malveillants.

En octobre 2008, Microsoft a publié une mise à jour critique de son système d'opération Windows (MS08-067). Cette mise à jour a pour but de réparer

une faille de sécurité permettant à un hacker de prendre le contrôle à distance d'un ordinateur vulnérable. Plusieurs familles de malware ont déjà intégrés ce nouveau mode de propagation pour infecter les ordinateurs. C'est le cas des familles Gimmiv et KernelBot.

La famille de malware que nous identifions sous le nom de GetCodec utilise aussi un nouveau mode de propagation: les fichiers multimédias. Cette famille n'exploite pas une vulnérabilité dans les lecteurs multimédias mais bien un mélange d'ingénierie

sociale et d'infection classique.

Quand un ordinateur est infecté, le malware balaie tout le disque dur et modifie les fichiers multimédias pour les transformer en format WMF. Il modifie ensuite l'entête des fichiers pour ajouter un lien vers un "codec" qui doit être téléchargé afin de lire le fichier. On aura deviné que le "codec" est en réalité une nouvelle variante de la famille "GetCodec".

Etant donné que plusieurs utilisateurs s'échangent des fichiers multimédias, nous avons recensé des centaines de milliers d'infections. GetCodec est toujours présent dans le décompte des dix menaces les plus actives.



# Bilan de l'année virale 2008

Par Pierre Marc Bureau, Chercheur en malware chez ESET



we protect your digital worlds



## Quelles attaques ont été les plus significatives cette année ?

Au cours de ces derniers mois, les attaques les plus significatives ont été celles menées à l'aide d'ingénierie sociale. Pour exemple, une famille de malware appelée Kryptic envoie un courrier électronique et prétend être un billet d'avion qui aurait été acheté ou une facture pour un service de livraison. Nous détectons des milliers de fichiers infectés de ce type chaque jour. De plus, les auteurs de ce malware créent quotidiennement de nouvelles variantes pour éviter d'être détectés par les logiciels antivirus. L'objectif de ce malware est d'installer d'autres composants malicieux tels que de faux antivirus.

Au cours de l'été 2008, un conflit s'est déclaré entre le gouvernement Géorgien et la Russie. Quelques heures à peine après le début des combats, nous avons observé des attaques massives sur Internet. Ces attaques provenaient des deux côtés de la frontière et avaient pour but de rendre inutilisable certains sites Internet jugés critiques, notamment ceux du gouvernement Géorgien et de différents médias en ligne. Il est probable que ce type d'attaque continuera d'accompagner les manœuvres militaires dans le futur et même avec encore plus d'ampleur.



## Quelles nouvelles menaces devraient émerger en 2009 ?

Les appareils mobiles gagnent toujours en popularité. Il est fort probable qu'un plus grand nombre d'attaques seront dirigées contre ces équipements dans les années à venir. En 2009, nous pensons être confrontés aux premières applications malveillantes pour l'iPod et recenser aussi une forte augmentation des attaques contre les communautés en ligne comme Facebook ou MySpace.

## Bilan de l'année 2008



Nous pensons que l'année 2008 a vu l'extinction du dernier réseau de zombie géant. Le réseau Storm ne semble plus être maintenu par ses auteurs. Ceux-ci ont vraisemblablement décidé de concentrer leurs efforts sur des opérations de plus petite envergure qui attirent moins l'attention des chercheurs et des journalistes. L'époque où deux ou trois gros réseaux de zombies se faisaient compétition avec des centaines de milliers d'ordinateurs infectés est révolue.

Même si les menaces évoluent, les moyens de défense pour les utilisateurs sont souvent les mêmes. Nous recommandons aux utilisateurs de s'assurer que tous leurs logiciels sont tenus à jour, autant leur système d'exploitation que leur lecteur multimédia et navigateur Internet. Nous recommandons aussi l'utilisation d'un logiciel antivirus à jour et une méfiance envers le contenu inconnu, reçu par courrier électronique ou visionné sur le web.

### ESET

Editeur des solutions  
ESET NOD32 Antivirus et  
ESET Smart Security

[www.eset.com](http://www.eset.com)

### ATHENA Global Services

Distributeur exclusif pour la France

[www.eset-nod32.fr](http://www.eset-nod32.fr)