



Communiqué de presse

## 34 millions de menaces identifiés par ESET en 2007, selon le Rapport annuel des menaces 2007

**ESET, éditeur de ESET NOD32 élu «Meilleur antivirus de l'année 2007» par AV-Comparatives, présente le Rapport annuel des menaces 2007  
Résumé de Pierre Marc BUREAU, Chercheur en malware**

Rapport annuel complet des menaces 2007 de Andrew LEE, Directeur Recherche et Développement chez ESET, en pièce jointe de ce communiqué.

Les Pavillons-sous-Bois – Le 19 février 2008

### Décompte des dix menaces les plus prévalentes dans les courriers électroniques

Au cours de cette année, les solutions ESET ont balayé plus de quatre milliards de messages. Parmi ceux-ci, près de 34 millions contenaient des fichiers malicieux, un record dans le monde des malwares.

Dix des menaces les plus détectées dans les courriers électroniques pour l'année 2007 sont les suivantes :

Nom du logiciel malicieux
A variant of Win32/Stration.WX worm
Probably unknown NewHeur_PE virus
Win32/Netsky.Q
Win32/Nuwar.gen worm
Win32/Fuclip.B trojan
Win32/Stration.XW worm
A variant of Win32/Stration.WL worm
Probably a variant of Win32/Nuwar worm
Win32/Stration.WC worm
A variant of Win32/Stration.QQ worm

« L'année 2007 nous a appris que le monde en ligne fourmille de logiciels malicieux et que les attaquants sont loin d'être en manque d'inspiration. Les vecteurs d'attaque sont très variés mais utilisent souvent la faiblesse humaine pour pénétrer les systèmes. », déclare Pierre Marc BUREAU, chercheur en malwares chez ESET.

« Ce décompte montre bien l'efficacité de notre détection proactive. La plupart des menaces détectées dans les communications électroniques l'ont été soit grâce aux heuristiques ou en établissant leur ressemblance avec des menaces connues. », poursuit Pierre Marc BUREAU.

### Les menaces qui ont marquées l'année 2007

De nouvelles menaces sont apparues au cours des derniers mois et certaines d'entre elles font d'ores et déjà parler d'elles.

#### Malware Mac

« À l'automne 2007, nous avons observé une des premières attaques visant autant les PCs utilisant Windows de Microsoft que les ordinateurs Apple qui utilisent le système d'exploitation OS X. Le vecteur d'infection de cette attaque est d'inciter une victime à télécharger et à installer un faux codec. », explique Pierre Marc BUREAU.

Le malware s'attaquant à OS X a un comportement semblable à celui de Win32/Zlob mais est beaucoup plus rudimentaire en comparaison des menaces avancées qui s'attaquent à Windows. Si un utilisateur

exécute ce fichier malicieux, il doit entrer son mot de passe administrateur pour que le malware puisse effectuer ses opérations malicieuses. La charge active du malware est de modifier la configuration de serveur de noms (DNS) de la victime, pour que toutes les requêtes DNS faites par un ordinateur infecté soient dirigées vers un serveur appartenant aux attaquants. Ce serveur peut ensuite être utilisé pour rediriger les visiteurs de sites bancaires vers des sites frauduleux utilisés pour voler ces informations sensibles.

### Faux codecs

Un des vecteurs d'infection les plus populaires en 2007 a été l'installation de faux codecs. Des pirates ont enregistré une multitude de sites web et les ont annoncés sur les sites de recherche comme Google et Yahoo. Les utilisateurs cherchant un "codec", c'est à dire un logiciel d'encodage et de décodage de flux vidéo, étaient dirigés vers ces sites malicieux.

Les utilisateurs qui acceptent de télécharger et d'exécuter les fichiers exécutables se trouvant sur ces sites infectent leurs ordinateurs avec une multitude de malware. La famille de malware Zlob est connue pour utiliser fréquemment cette technique d'ingénierie sociale comme vecteur d'infection.

### Nuwar (Storm Worm)

Ce logiciel malicieux a énormément attiré l'attention des média en 2007. Son nom (Storm Worm), provient de la première grande campagne de SPAM qui a été menée pour le distribuer au mois de janvier en référence à la tempête Kyrill. Il y a plusieurs raisons pour cet attrait médiatique. Premièrement, cette menace est l'une des premières à utiliser un réseau P2P pour sa communication de commande et contrôle. Le fait que Nuwar utilise un réseau décentralisé pour communiquer fait en sorte qu'il est très difficile pour la communauté de chercheurs d'évaluer le nombre de systèmes qui ont été infectés.

*« Certains chercheurs affirment que plus d'un million de systèmes auraient été infectés alors que les chercheurs de Microsoft affirment n'en avoir observé que quelques centaines de milliers. Notre solution antivirus détecte cette menace sous le nom de Nuwar et Fuclip. Le nom de Nuwar est attribué au composant principal tandis que Fuclip est le nom de la détection pour la composante responsable de camoufler l'infection. »,* ajoute Pierre Marc BUREAU.

Andrew LEE et Pierre Marc BUREAU, membres de l'équipe de recherche d'ESET, ont publié un article sur ce malware dans l'édition de novembre de la revue Virus Bulletin.

### Prédictions pour l'année 2008

L'étude réalisée par ESET permet d'avancer quelques prédictions pour l'année 2008 :

- Les réseaux de systèmes infectés (botnets) comme celui de Nuwar continueront à diversifier leurs mécanismes de communication et à s'étendre.
- Il y aura plus de spams dans les boîtes aux lettres en 2008 qu'en 2007.
- Les technologies du Web 2.0 gagneront en popularité et attireront d'avantage l'attention des attaquants.
- Les jeux en ligne et communautés virtuelles comme Second Life subiront plus d'attaques.
- ESET continuera d'offrir une protection à la pointe de la technologie à ses clients !

Téléchargez le rapport des menaces 2007 dans son intégralité :  
[http://www.eset-nod32.fr/PDF/presse/eset\\_global\\_threats\\_reports\\_2007.pdf](http://www.eset-nod32.fr/PDF/presse/eset_global_threats_reports_2007.pdf)

**Pour toute demande d'interview, merci de contacter Elektron**

**Agence Elektron Relation Presse**  
Mélanie JAPAUD / Hélène HARRIET  
Tel. : 01.45.26.01.04  
Mail : [japaud@elektron-presse.com](mailto:japaud@elektron-presse.com)

**Athena Global Services**  
Laetitia BONNOT  
Tel. : 01.55.89.08.84  
Mail : [laetitia.b@athena-gs.com](mailto:laetitia.b@athena-gs.com)

## **A propos d'ESET**

La société ESET est spécialisée dans la conception et le développement de logiciels de sécurité offrant une protection globale contre les menaces évolutives qui sévissent dans les environnements informatiques. Pionnier en matière de détection proactive des menaces, ESET est aujourd'hui le leader dans ce domaine. ESET a développé un vaste réseau mondial de partenariats, y compris avec des entreprises telles que Canon, Dell et Microsoft. ESET possède des bureaux à Bratislava (Slovaquie), Bristol (Royaume-Uni), Buenos Aires (Argentine), San Diego (USA), Prague (République Tchèque), et est représenté dans plus de 110 pays.

Pour plus d'informations : [www.eset.com](http://www.eset.com)

## **A propos d'Athena Global Services**

Créée en 1997, ATHENA Global Services est une entreprise indépendante spécialisée dans la distribution de logiciels de sécurité informatique. A travers un vaste réseau de distribution, constitué de VAR, revendeurs locaux professionnels et des plus importantes enseignes spécialisées dans la distribution de logiciels, Athena Global Services propose des logiciels et équipements de sécurité novateurs destinés aux particuliers et aux entreprises, pour protéger et gérer leur environnement informatique : antivirus, pare-feu, chiffrement, politique de sécurité, authentification, sauvegarde, migration des données, et contrôle du trafic Internet. En outre, ATHENA Global Services propose une gamme de logiciels utilitaires également dédiés à la protection et à l'optimisation des parcs informatiques. Grâce à son savoir-faire, ATHENA Global Services entretient des relations privilégiées avec les éditeurs mondiaux qui lui confient la localisation et la distribution de leurs logiciels.

Pour en savoir plus, veuillez visiter les sites Internet : [www.eset-nod32.fr](http://www.eset-nod32.fr) ou [www.athena-gs.com](http://www.athena-gs.com)