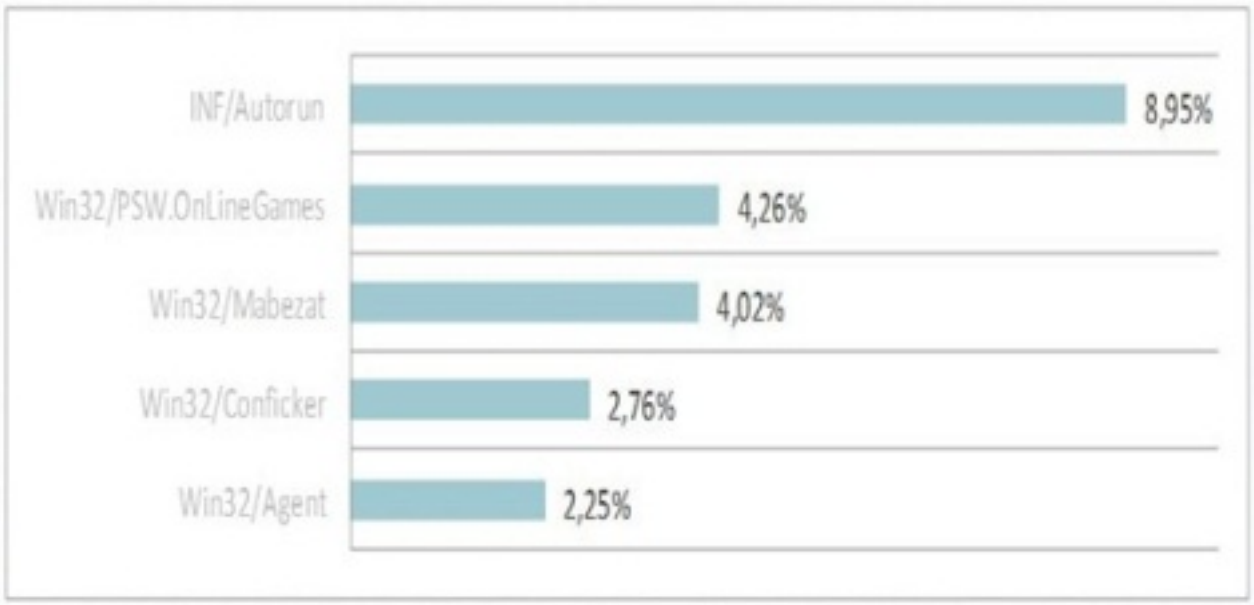
***Sécurité : Les menaces identifiées par ESET en France : Mars 2010***
**Sécurité**
Posté par : JulieM
Publiée le : 9/4/2010 15:00:00

**INF/autorun apparaît encore une fois en première position**. Avec un taux de 8,95%, INF/Autorun maintient sa présence en tête de liste des menaces subies par les postes de travail en France

Cette menace se manifeste à travers les médias amovibles. En modifiant le contenu du fichier d'instruction autorun.inf, elle permet l'exécution automatique du malware lors de l'insertion des medias infectés dans le système.

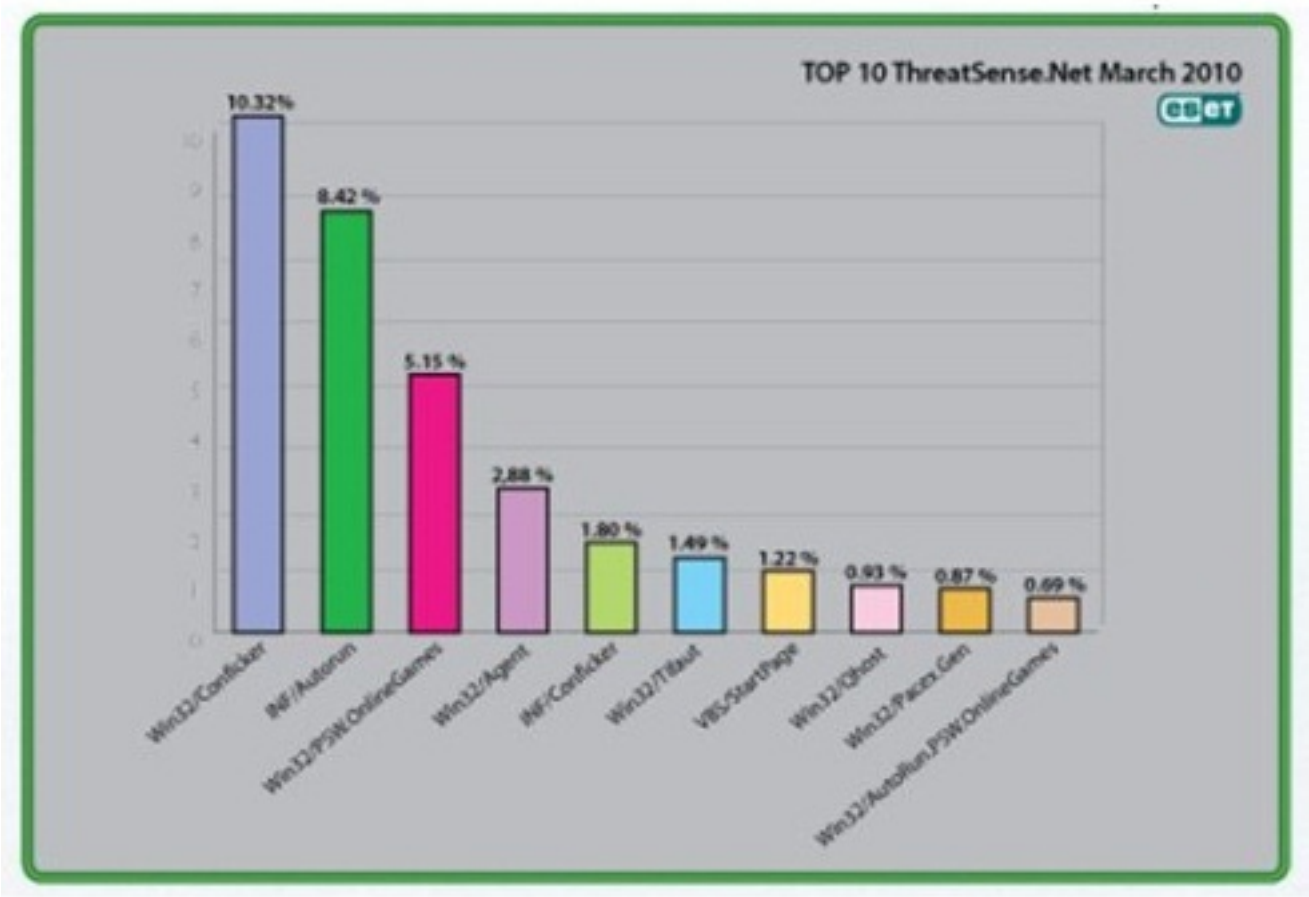
Les résultats de cette analyse statistique sont basés sur le moteur ThreatSense.Net® qui opère en mode "cloud computing" en recueillant des données soumises par les utilisateurs qui emploient ESET Smart Security and ESET NOD32 Antivirus partout dans le monde.




**En seconde position on retrouve le troyen Win32/PSW.Online Games**. Comme son nom l'indique, Win32/PSW.OnlineGames attaque les utilisateurs de jeux en ligne, en tentant de récupérer les identifiants et mots de passe lors de la connexion. Win32/Mabezat arrive en troisième position, avec un taux de 4,02%, suivi par Win32/Conficker (2,76%). Enfin, la cinquième position est occupée par un type de menace intitulée Win32/Agent. Elle couvre un large éventail de malwares Internet entrant dans la catégorie des vols de données sensibles. En mars, Win32/Agent a atteint les 2,25% de toutes les détections de malwares.

L'Europe est menacée par la propagation d'un troyen

**Le moteur ThreatSense.Net® d'ESET** qui collecte les malwares de toute l'Europe, a connu une recrudescence d'activité au mois de mars suite à la propagation du troyen Win32/Lethic.AA. Pour l'instant, cette menace touche principalement les pays du nord et de l'est de l'Europe.




Le Troyen est utilisé pour la distribution de Spams et il peut être contrôlé à distance. Pour infiltrer l'ordinateur d'un utilisateur, Win32/Lethic.AA véhicule probablement un autre malware ou est téléchargé dans l'ordinateur de l'utilisateur par un malware déjà présent. Le but principal de ce Troyen est de transformer l'ordinateur infecté en composant d'un Botnet (réseau de PC) puissant pour la diffusion de mails indésirables. Pour éviter d'être détecté, son code de programmation est inclus dans le fichier ''**explorer.exe**''. Pour combattre ce troyen, ESET recommande d'effectuer régulièrement les mises à jour des navigateurs Internet et des logiciels de sécurité avec un maximum de précaution lors du téléchargement de fichiers et dans la navigation sur Internet.

Vous trouverez les solutions de protection Eset chez notre partenaire, **EptiSoft**, le Magasin en ligne spécialisé dans la vente de produits dématérialisés et **c'est à cette adresse**