

Rapport mensuel des menaces identifiées par ESET en France :

Mars 2010

– 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.

Principales menaces d'ordinateurs en France selon ESET ThreatSense.Net® (mars 2010)

D'après l'analyse de ThreatSense. Net[®] d'ESET, la menace Win32/Conficker arrive en tête du TOP 10 mondial, ce mois-ci avec près de 10,32 % du total général des menaces.

À propos de ThreatSense. Net[®]

ThreatSense.Net[®] collecte de façon anonyme des informations statistiques sur les différents types d'infiltrations détectées sur les postes de travail des utilisateurs. Grâce à cette information, le laboratoire d'ESET dispose d'informations précises et en temps réel, sur les infiltrations les plus répandues. Les infiltrations détectées par l'analyse heuristique sont alors répertoriées avec la mise à jour des contre-attaques des malwares émis, avant qu'il puisse se propager ou muter dans une variante différente.

À 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

À propos d'Athena Global Services

Créée en 1997, ATHENA Global Services est une entreprise indépendante spécialisée dans la distribution de logiciels de sécurité informatique. À 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.com nod32.fr ou www.athena.com gs.com