



Contacts Presse

ATHENA Global Services
20 allée Louis Calmanovic
93320 Les Pavillons-sous-bois,
Tel : 01 55 89 08 84
Fax : 01 55 89 08 89
Laëtitia Bonnot
laetitia.b@athena-gs.com

InterPresse

Parc de Garlande
1 rue de l'Égalité
92000 Bagneux
Tel : 01 55 48 05 10
Fax : 01 55 48 05 11
Isabelle Guillou
iguillou@interpresse.fr
Norbert Spitéri
nspiteri@interpresse.fr

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 le site Internet : www.athena-gs.com

COMMUNIQUE DE PRESSE

2 Février 2010

Les chercheurs d'ESET prévoient une recrudescence des menaces d'ingénierie sociale en 2010

Les Pavillons-sous-Bois, le 2 février 2010. Eset, spécialiste de la conception et du développement de logiciels de sécurité, dresse un portrait des actes de malveillances probables en 2010, touchant les équipements connectés à l'Internet. Après avoir effectué un bilan des menaces constatées en 2009 et analysé les tendances observées ces derniers mois, les chercheurs d'ESET ont établi une liste d'attaques prévisibles, par ordre d'importance, qui affecteront principalement les internautes.

En tout premier lieu, ESET anticipe une forte progression des menaces d'ingénierie sociale. Ce type de cybercriminalité consiste à tromper les utilisateurs sous de faux noms (usurpation de sites légitimes notamment) pour récupérer des données personnelles à travers la messagerie internet, le téléphone fixe ou mobile ou les Smartphones.

Eset met en garde les utilisateurs et les entreprises face aux solutions de Cloud Computing qui déportent la sécurité des applications chez l'hébergeur. Eset recommande également une extrême vigilance envers les faux logiciels de sécurité qui introduisent généralement un cheval de Troie.

Voici un résumé des conclusions des experts d'ESET :

1. Les attaques d'ingénierie sociale continueront à prédominer, alors que les attaques basées sur les vulnérabilités des systèmes d'exploitation continueront à diminuer du fait que de plus en plus de personnes vont se tourner vers des OS plus sécurisés. Bien que les vulnérabilités dans les applications restent une menace sérieuse, elles tendront à se réduire car les éditeurs améliorent leur contrôle qualité et la méthodologie des correctifs. Windows 7 contribuera à réduire la progression du malware INF/Autorun.
2. Des occasions comme les jours fériés, des nouvelles (vraies ou fabriquées), des événements populaires, comme la coupe du monde et des préoccupations persistantes, telles que la crise économique nationale et mondiale, seront utilisées comme opportunité pour des attaques d'ingénierie sociale.
3. Bien que les attaques Jailbroken pour l'iPhone vont affecter moins de personnes, la menace sur les mobiles va s'amplifier, notamment à travers l'ingénierie sociale comme décrit ci-dessus.
4. Il y aura davantage de cas où des propriétaires de systèmes infectés mettront du temps à trouver une solution réparatrice.
5. Les infractions de données continueront à se développer et l'efficacité de la sécurité mise en œuvre dans les solutions de Cloud computing, au moins à court terme, va considérablement changer la donne.
6. Il y aura plus d'escroqueries provoquées par les logiciels rogues et l'ampleur des fraudes est susceptible de s'élargir grâce aux faux logiciels de sécurité.
7. "Malware as a service" deviendra de plus en plus un modèle coopératif entre les spécialistes de la cybercriminalité.



8. Il y aura probablement un usage plus fréquent de codes malveillants écrits avec des langages de programmation de haut niveau à travers des plates-formes multiples.
9. Des réseaux sociaux seront visés davantage par des attaques d'ingénierie sociale et seront l'objet d'investigation en termes de vulnérabilités.
10. Il y aura davantage de tentatives d'attaques dans les environnements virtualisés, bien que leur efficacité soit susceptible d'être limitée.
11. Le Phishing et les attaques associées sur des jeux en ligne continueront de représenter une menace très importante, cependant les attaques sur les consoles de jeu n'auront qu'un effet limité.
12. Les attaques concernant les connexions sans-fil continueront de fleurir.
13. Les criminels et les entreprises légitimes seront attentifs aux données personnelles disséminées sur de multiples ressources exploitant l'interopérabilité entre les fournisseurs de réseaux sociaux. Le partage des données dans le secteur privé constituera une menace croissante jusqu'à ce que le besoin de règles plus strictes, en matière de protection des données, s'imposera comme on peut le constater dans les services publics en Europe.
14. L'escroquerie à grande échelle sera la forme la plus commune de malwares, en raison de son potentiel de gains importants.
15. L'usurpation de sites Web légitimes et de réseaux sociaux comme vecteur d'attaques continuera à proliférer. Nous sommes susceptibles de voir plus d'utilisation de tels réseaux comme des moyens de gérer les infrastructures illicites employées par les réseaux organisés (tels que les botnets).
16. Des attaques ciblées de type spear-phishing et whaling seront monnaies courantes, alors que ces menaces seront sous-estimées.

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-Unis), Buenos Aires (Argentine), San Diego (USA), Prague (République Tchèque), et est représenté dans plus de 110 pays. Pour plus d'informations, veuillez visiter les sites Internet : www.eset-nod32.fr ou www.athena-gs.com