COMMUNIQUÉ DE PRESSE **5 septembre 2013**

ESET découvre un cheval de Troie bancaire baptisé "Hesperbot" affectant notamment les plates-formes Android en Europe et en Turquie

Les Pavillons-sous-Bois, le 5 septembre 2013, ESET, acteur mondial de la protection proactive depuis 25 ans, Le laboratoire principal de recherche d'ESET a découvert un nouveau cheval de Troie bancaire qui cible les utilisateurs de services bancaires en ligne en Europe et en Asie. Utilisant une apparence très crédible de campagnes liées à des organisations dignes de confiance, il incite les victimes à exécuter des logiciels malveillants. Plusieurs victimes ont déjà été dépouillées de leurs avoirs à cause de cette menace nouvellement révélée. Sur la base de données LiveGrid ® - système de collecte des logiciels malveillants basés sur le Cloud d'ESET - des centaines d'infections ont été détectées en Turquie, des dizaines en République tchèque, au Royaume-Uni et au Portugal. Ce malware bancaire très puissant et sophistiqué baptisé Hesperbot se propage par e-mails sous forme de phishing et tente d'infecter les appareils mobiles fonctionnant sous Android, Symbian et Blackberry.

Référencé comme Win32/Spy.Hesperbot, cette menace intègre des fonctionnalités de keylogger, peut effectuer des captures d'écran fixe ou de vidéo et mettre en place un proxy distant. Il comporte également quelques astuces plus avancées, telles que la création d'une connexion à distance cachée pour le système infecté. « *L'analyse de la menace a révélé que nous avions affaire à un cheval de Troie bancaire, avec des fonctionnalités similaires et des objectifs identiques au fameux malware Zeus et SpyEye, mais les différences d'installation sont importantes, laissant entendre qu'il s'agit d'une nouvelle famille de logiciels malveillants, et non d'une variante d'un cheval de Troie déjà connu,* » explique Robert Lipovsky, chercheur en malware d'ESET qui dirige l'équipe d'analyse de cette menace. « *Les solutions d'ESET telles que ESET Smart Security et ESET Mobile Security protègent contre ce malware* », at-il ajouté .

Les Cybercriminels visent à obtenir des informations de connexion leur permettant d'obtenir les codes d'accès au compte bancaire de la victime et de les amener à installer un composant mobile du malware sur leur téléphone Symbian, Blackberry ou Android.

La campagne de malware a commencé en République Tchèque le 8 Août 2013. Les auteurs ont enregistré le domaine www.ceskaposta.net, qui est très ressemblant au site actuel de la Poste tchèque. *« Ce n'est pas surprenant que les assaillants aient essayé de leurrer les victimes potentielles en les incitant à ouvrir les logiciels malveillants via des emails de phishing, apparaissant comme des informations de suivi de colis de la Poste. Cette technique a été utilisée de nombreuses fois auparavant* » , précise Lipovsky. Le service postal tchèque a réagi très rapidement en émettant un avertissement sur l'escroquerie, via leur site web .

Néanmoins, le pays le plus touché par ce cheval de Troie bancaire est la Turquie, avec une détection de ce malware a une date antérieure au 8 Août. De récents pics d'activité de botnet ont été observés en Turquie en juillet 2013, mais ESET a également repéré des échantillons plus anciens qui remontent au moins à avril 2013. L'e -mail de phishing qui a été envoyée aux victimes potentielles ressemble à une facture. Une variante du malware a également été trouvée sur la toile, conçue pour cibler les utilisateurs d'ordinateurs au Portugal et au Royaume-Uni .

Une analyse plus détaillée de ce malware est disponible en blogpost sur WeLiveSecurity.com, la nouvelle plate-forme d'ESET qui analyse et commente les cyber-menaces et donne des conseils de sécurité utiles. Voir le lien ci-après :

http://www.welivesecurity.com/2013/09/04/hesperbot-a-new-advanced-banking-trojan-in-the-wild/

Sur WeLiveSecurity.com vous trouverez prochainement un suivi sur cette menace et un livre blanc sur le malware Hesperbot.

À propos d'ESET
Fondée en 1992, la société ESET est spécialisée dans la conception et le développement de logiciels de sécurité pour les entreprises et le grand public. Pionnier en matière de détection proactive des menaces véhiculées par l'Internet depuis 25 ans, ESET est aujourd'hui l'un des leaders dans ce domaine. En obtenant la 80ème récompense VB100 en juin 2013, ESET NOD32 Antivirus détient le record mondial pour le nombre de récompenses Virus Bulletin (VB100), et n'a jamais manqué un seul ver ou virus «In-the-Wild" depuis le début des tests en 1998. ESET a été reconnue comme l'une des entreprises les plus innovantes en Europe pour 2011 au titre des HSBC European Business Awards et a été primée maintes fois par les laboratoires AV-Comparatives, AVTest et bien d'autres encore.
ESET NOD32, ESET Smart Security et ESET Cybersecurity pour Mac sont reconnus et appréciés par des millions d'utilisateurs dans le

monde.
ESET a son quartier général à Bratislava (Slovaquie), possède des filiales à San Diego (U.S.), Buenos Aires, et Singapour et des bureaux à Jena (Allemagne), Sao Paulo et Prague. Ses centres de recherche sont établis à Bratislava, San Diego, Buenos Aires, Singapour, Prague, Košice (Slovaquie), Cracovie (Pologne), Montréal et Moscou. ESET est également représenté dans plus de 180 pays à travers un réseau de partenaires.

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 le site Internet : www.athena-gs.com

Contact Presse
InterPresse - Norbert Spitéri - nspiteri@interpresse.fr - Tél : 01 45 87 80 54 / 06 60 91 97 49