COMMUNIQUÉ DE PRESSE 18 février 2013

16.000 comptes Facebook piratés.

ESET a découvert un cheval de Troie qui a dérobé les informations de connexion de plus de 16.000 comptes Facebook

Les Pavillons-sous-Bois, le 18 février 2013, ESET, acteur majeur en matière de protection proactive, a découvert un cheval de Troie d'ingénierie sociale. Le malware a réussi à voler les identifiants de connexion de plus de 16.000 utilisateurs Facebook. L'objectif du malware était de récupérer ces informations et de les lier aux statistiques utilisateurs des joueurs de Texas HoldEm Poker (jeu de Poker gratuit accessible en ligne via FB). Les systèmes de détection d'ESET ont montré que la menace s'est propagée presque exclusivement en Israël. A noter que l'application cible est fondée sur un logiciel légitime et très populaire signé de l'éditeur Zynga Inc. Selon le site de référence des applications Facebook AppData, ce jeu de poker dispose d'une audience mensuelle de 35 millions d'utilisateurs actifs.

ESET a commencé à étudier ce cheval de Troie début 2012. Cependant, grâce à une détection générique proactive de cette menace, les utilisateurs de solutions de sécurité ESET ont été protégés contre ce malware depuis fin 2011. Comme les statistiques de détection ont montré que la menace était diffusée principalement en Israël, ESET a contacté l'organisme israélien CERT (Computer Emergency Response Team) ainsi que la police israélienne début 2012. Pendant l'enquête, ESET ne pouvait pas fournir publiquement de détails sur cette menace, mais aujourd'hui le malware a été désactivé.

L'attaquant a utilisé le logiciel malveillant pour obtenir des informations d'identification de l'utilisateur lors de l'ouverture de la session Facebook, son score dans le jeu, ainsi que des informations sur le montant en cartes de crédit enregistré dans ses paramètres Facebook et disponible pour augmenter sa mise dans le jeu de poker. Le jeu possède une fonctionnalité qui permet la reconstitution de la valeur du jeton en argent réel en saisissant les détails de la carte de crédit ou du compte PayPal. Pour obtenir des informations d'identification d'utilisateurs, une armée de 800 ordinateurs a été utilisée - tous infectés et contrôlés par l'attaquant. Ces machines ont exécutés des commandes à partir du serveur de C & C (Command & Control). Le créateur de la menace a lancé une attaque en utilisant les identifiants de connexion de plusieurs comptes FB, qui ont été acquis à l'avance.

« Pour se protéger contre des attaques reposant sur des méthodes d'ingénierie sociale, une bonne solution de sécurité n'est pas suffisante. Les utilisateurs doivent rester vigilant face à toutes formes de stratagèmes comme celui-ci », déclare Robert Lipovsky, responsable de l'équipe ESET Security Intelligence. Il ajoute « L'utilisateur doit pouvoir reconnaître la fausse page de connexion FB en vérifiant l'adresse URL du site. »

Les ordinateurs infectés ont reçu une commande pour ouvrir une session dans les comptes FB de l'utilisateur et acquérir un score utilisateur du jeu Texas HoldEm, ainsi que la quantité de cartes de crédit enregistrées dans son compte FB. Dans le cas d'un utilisateur avec une carte de crédit affichant un faible score, l'ordinateur infecté reçoit des instructions pour infecter le profil de la victime FB avec un lien vers un site de phishing. Ce site a agi directement ou indirectement pour attirer les amis du joueur FB vers un site ressemblant à la page d'accueil FB. Dans le cas où les informations d'identification ont été saisies par eux, elles ont également été récoltées par l'attaquant. Lors de l'analyse de ce botnet, ESET estime que l'attaquant a pu accéder à un total de 16.194 identifiants de connexion. ESET souhaite mettre en garde la communauté FB sur la probabilité que d'autres applications FB auraient pu être infectées de cette manière, pas seulement ce jeu de poker.

Le nombre de menaces véhiculées par Facebook est en pleine expansion. Pour contrer cette tendance, ESET a mis en place une application de sécurité d'analyse des médias sociaux ESET Social Media Scanner disponible gratuitement en ligne, qui est capable de scanner le profil de l'utilisateur pour repérer la présence de liens malveillants et de phishing. De plus, l'application permet de détecter des liens malveillants sur la timeline d'amis Facebook de l'utilisateur.

Pour plus d'informations, connectez-vous sur le site : www.eset.com/fr

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, ESET est aujourd'hui l'un des leaders dans ce domaine. En obtenant la 75ème récompense VB100 en septembre 2012, 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 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