COMMUNIQUÉ DE PRESSE **18 décembre 2013**

Un Cheval de Troie bancaire capable de contourner le processus d'authentification, cible des utilisateurs en France, aux Pays-Bas et en Italie.

Les Pavillons-sous-Bois, le 18 décembre 2013. Le laboratoire de recherche d'ESET implanté à Montréal vient de détecter un logiciel malveillant sous forme d'un cheval de Troie bancaire très actif, baptisé Qadars. Ce code malveillant cible principalement les utilisateurs de différents pays dont la France, les Pays-Bas, l'Italie, le Canada, l'Inde et l'Australie. Qadars utilise une grande variété de "WebInjects", c'est à dire d'injection de contenu HTML et/ou javascript dans une page. Certaines injections intègrent des composants destinées aux mobiles sous Android qui sont capables de contourner les systèmes d'authentification à deux facteurs de la banque en ligne afin d'avoir accès au compte bancaire de l'utilisateur. Le cheval de Troie identifie les utilisateurs dans des régions spécifiques et utilise des fichiers de configuration d'injections web adaptés aux banques les plus couramment utilisés par les victimes, ce qui le rend beaucoup plus efficace. « *Le malware a été observé par ESET lors des six derniers mois et nous pouvons confirmer qu'il est constamment mis à jour* », indique Jean-Ian Boutin, chercheur chez ESET Canada.

Détecté comme Win32/Qadars, le malware utilise un schéma « Man-in-the-Browser » pour effectuer la fraude financière. Le virus s 'injecte dans les processus du navigateur (Firefox ou Internet Explorer) et est capable d'in sérer du contenu dans les pages consultées par l'utilisateur. Certaines des injections sont très sophistiquées et peuvent effectuer des opérations automatiquement et contourner les systèmes d'authentification à deux facteurs mis en œuvre par les banques.

« *Le contenu peut revêtir plusieurs formes, mais il possède généralement une aptitude à récolter des informations d'identification de l'utilisateur ou à manipuler le code JavaScript afin de tenter des transferts d'argent automatiques, sans que l'utilisateur s'en aperçoive et sans son consentement* », explique Jean- Ian Boutin. « *Les fichiers de configuration des "WebInjects" du malware Qadars changent fréquemment et ciblent des organismes spécifiques. Pour maximiser leur succès, les auteurs de ces logiciels malveillants essaient d'infecter les utilisateurs dans des régions spécifiques du monde* » , ajoute Jean- Ian Boutin.

Une analyse plus détaillée de ce malware est disponible dans le blog d'ESET sous le nom de Qadars sur le site WeLiveSecurity.com.

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 26 ans, ESET est aujourd'hui l'un des leaders dans ce domaine. En obtenant la 81ème récompense VB100 en août 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.

Ses principaux partenaires éditeurs de solutions de sécurité :
DeviceLock - ESET Antivirus - StorageCraft - WebSure - SMSPasscode - 8Man - WhiteCanyon - EndSec Cloud Services - MDM

Ainsi que ses filiales Africa Global Services - Auxiliance - Marketing Land

Pour en savoir plus, veuillez visiter le site Internet : www.athena-gs.com

Contacts Presse
Athena Global Services - Marion Lecrique - marion.l@athena-gs.com - 01 55 89 09 60
InterPresse - Norbert Spitéri - nspiteri@interpresse.fr - Tél : 01 45 87 80 54 / 06 60 91 97 49