COMMUNIQUÉ DE PRESSE 21 mars 2012

ESET alerte sur l'apparition d'un botnet très élaboré qui entame son voyage de Georgie vers la France.

Les Pavillons-sous-Bois, le 21 mars 20122 - Au début de cette année, les chercheurs d'ESET, société éditrice du célèbre NOD32 Antivirus et leader en matière de protection proactive, avaient découvert un botnet ayant des fonctionnalités de communication uniques. En plus d'autres activités, le botnet en question tente de voler des documents et certificats, peut créer des enregistrements audio et vidéo et scanner tout un réseau local à la recherche d'informations. Une autre caractéristique surprenante est qu'il recherche des fichiers de configuration de « Bureau à distance », ce qui permet aux pirates de voler des informations sur des machines distantes sans exploiter de failles. Cette menace s'appuie sur un site gouvernemental Georgien pour mettre à jour ses informations de C&C (Command and Control), c'est pourquoi les chercheurs d'ESET pensent qu'initialement W32/Georbot ciblait les ordinateurs de ce pays. Plus inquiétant encore, ce malware est toujours en développement car ESET a d'ores et déjà identifié des variantes récentes ; notamment une datant du 20 mars et qu'il commence à se répandre en dehors de la Georgie, en France notamment.

Pays	Taux de pénétration
Georgie	70,45 %
État- Unis	5,07 %
Allemagne	3,88 %
Russie	3,58 %
Canada	1,49 %
Ukraine	1,49 %
France	1,19 %
Autres	12,83 %

W32/Georbot a la capacité de se mettre à jour pour se métamorphoser en une nouvelle version, ce qui lui permet de ne pas être détecté par les scanners anti-malware. Ce botnet peut également se mettre en repli s'il n'arrive pas à atteindre le serveur de commande et dès lors se connecter à une page Internet spéciale hébergée sur un serveur appartenant au gouvernement Georgien. « *Ceci n'implique pas nécessairement que le gouvernement Georgien soit en cause. La plupart du temps, les propriétaires de sites web ne savent pas que leurs systèmes sont compromis* » indique Pierre-Marc Bureau, Manager d'ESET Security Intelligence. Ce dernier ajoute « *Il est également important de noter que le Ministère de la Justice Georgien et le CERT local sont au courant de la situation et collaborent avec ESET sur ce sujet* ». Sur l'ensemble des infections recencées, 70% étaient localisées en Georgie, suivi par les Etats-Unis, l'Allemagne et la Russie, la France faisant également partie du top 7 des pays concernés.

Les chercheurs d'ESET ont également réussi à accèder au panneau de contrôle du botnet , permettant ainsi d'obtenir beaucoup de détails sur le nombre d'ordinateurs touchés, leur localisation et les commandes possibles. L'information la plus intéressante trouvée est la liste des mots-clés ciblés dans les documents des systèmes infectés. Parmi les nombreux termes anglais figuraient notamment « ministère, service, secret, agent, USA, Russie, FBI, CIA, arme, FSB, KGB, téléphone, numéro. »

Contacts Presse

ATHENA Global Services
Tel : 01 55 89 08 84
Laëtitia Bonnot
laetitia.b@athena-gs.com

InterPresse
Norbert Spitéri
nspiteri@interpresse.fr
01 45 87 80 54
06 60 91 97 49

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

« *La fonction d'enregistrement vidéo via la webcam, la prise de capture d'écrans et le lancement d'attaques DDoS (attaques par deni de service) ont été utilisés à plusieurs reprises » précise* P-M Bureau. Le fait que ce botnet utilise un site Georgien pour mettre à jour ses informations de contrôle et de commande, et qu'il utilise probablement le même site pour se répandre, indique que la population Georgienne est sa cible principale. Malgré son pouvoir de nuisance important, le niveau de sophistication de ce botnet n'est pas suffisant pour penser qu'il ait pu être à l'initiative d'un état. Dans ce cas de figure, elle aurait été probablement plus professionnelle et plus discrète, selon les chercheurs d'ESET. L'hypothèse la plus probable est que W32/Georbot a été créé par un groupe de cybercriminels à la recherche d'informations sensibles afin de les revendre à d'autres organisations.

« *La cybercriminalité tend à se professionnaliser et à devenir plus ciblée. W32/Stuxnet et W32/Duqu sont de bons exemples de menaces de haut-niveau ayant des finalités bien précises. En revanche, même si ce malware semble moins sophistiqué, W32/Georbot intègre de nouvelles méthodes et fonctionnalités originales pour accéder au cœur de ce que recherchent ses créateurs. Dans le cas de W32/Georbot, c'est la recherche d'informations spécifiques, d'accès aux systèmes et de fichiers de configuration de 'Bureau à distance'»* conclu Righard Zwienenberg, Directeur de recherche chez ESET.

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 le leader dans ce domaine. À ce jour, l'antivirus ESET Nod32 détient le record mondial de récompenses décernées par le laboratoire indépendant Virus Bulletin depuis 1998. 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) et possède des filiales à San Diego (U.S.), Buenos Aires, et Singapour. Ses centres de recherche sont établis à Bratislava, San Diego, Buenos Aires, Prague, Cracovie, Montréal et Moscou. ESET est également représenté dans plus de 180 pays à travers un réseau de partenaires.

Pour plus d'informations, veuillez visiter les sites Internet : www.eset-nod32.fr ou www.athena-gs.com