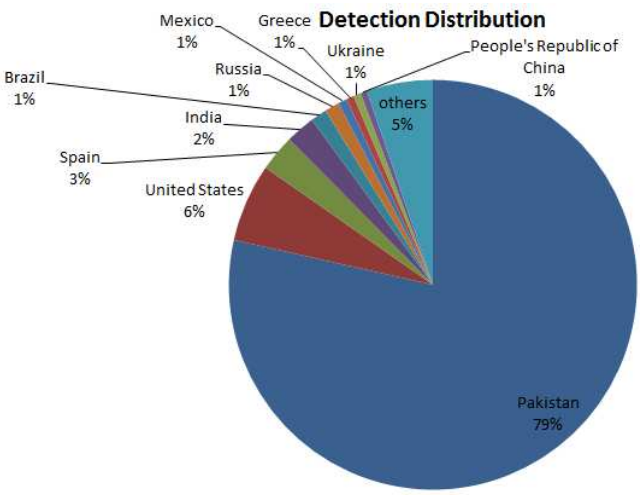
COMMUNIQUÉ DE PRESSE 17 mai 2013

ESET révèle une cyber-attaque principalement orientée vers le Pakistan à travers de faux documents PDF attachés.

Les Pavillons-sous-Bois, le 17 mai 2013. ESET, pionnier en matière de sécurité proactive depuis 25 ans, a découvert et analysé une cyber-attaque ciblée qui tente de voler des informations sensibles provenant de différentes organisations, notamment au Pakistan (avec une portée limitée dans le monde). Au cours de cette investigation menée par ESET, plusieurs pistes ont été découvertes qui indiquent que la menace est d'origine indienne et qu'elle sévit depuis au moins deux ans.

Cette attaque ciblée a utilisé un certificat de signatures de code délivré par une société apparemment légitime qui aurait produit des signatures binaires malveillantes et favorisé leur potentiel de propagation. La société est basée à New Delhi et le certificat a été délivré en 2011. Le malware se diffuse à travers des pièces jointes aux e-mails.

« *Nous avons identifié plusieurs documents différents qui évoquent plusieurs thèmes susceptibles d'être attractifs pour les bénéficiaires. L'un d'eux concerne les forces armées indiennes. Nous n'avons pas d'informations précises quant aux personnes ou organisations qui ont été plus particulièrement touchées par ces fichiers, mais sur la base de nos enquêtes, nous formulons l'hypothèse que des personnes et des institutions au Pakistan ont été ciblées »,* a déclaré Jean-Ian Boutin, chercheur en malware chez ESET. Par exemple, l'un des fichiers PDF frauduleux a été diffusé par une archive auto-extractible appelée "pakistandefencetoindiantopmiltrysecreat.exe", et le système de supervision d'ESET montre que le Pakistan est fortement affecté par cette campagne avec 79 % des détections repérées dans ce pays.



Le premier vecteur de l'infection exploite une vulnérabilité largement utilisée et connue sous le nom CVE-2012-0158. Cette vulnérabilité peut être exploitée par des documents Microsoft ® Office spécialement conçus qui permettent l'exécution de code arbitraire. Les documents ont été transmis par email et le code malveillant s'exécute dès que le document est ouvert, sans que l'utilisateur de l'ordinateur attaqué s'en aperçoive. L'autre vecteur d'infection s'effectue via les fichiers exécutables Windows qui apparaissent comme des documents Word ou PDF diffusés par la messagerie. Dans les deux cas, pour échapper à la suspicion de la victime, de faux documents sont présentés à l'utilisateur lors de l'exécution.

Le malware a volé des données sensibles à partir d'ordinateurs infectés et les a envoyées vers les serveurs des attaquants. Il a utilisé différentes techniques de vols de données, parmi elles un keylogger, réalisant des captures d'écran et envoyant des documents de l'ordinateur infecté vers le serveur de l'attaquant. Fait intéressant, les informations volées à partir d'un ordinateur infecté ont été téléchargées vers le serveur de l'attaquant sans cryptage. "La décision de ne pas utiliser de cryptage est étonnante dans la mesure où cette opération est relativement simple à utiliser et aurait pu masquer davantage l'opération», ajoute Jean-Ian Boutin.

Une analyse technique complète est disponible sur le site WeLiveSecurity.com – la nouvelle plate-forme d'ESET dédiée à l'analyse des cyber-menaces et aux conseils de sécurité.

Noms de détection

C'est une menace multi-partie et multi-vectorielle, dont les noms des menaces attribués par ESET sont les suivants :

Win32/Agent.NLD worm
Win32/Spy.Agent.NZD Trojan
Win32/Spy.Agent.OBF Trojan
Win32/Spy.Agent.OBV Trojan
Win32/Spy.KeyLogger.NZL Trojan
Win32/Spy.KeyLogger.NZN Trojan
Win32/Spy.VB.NOF Trojan
Win32/Spy.VB.NRP Trojan
Win32/TrojanDownloader.Agent.RNT Trojan
Win32/TrojanDownloader.Agent.RNV Trojan
Win32/TrojanDownloader.Agent.RNW Trojan
Win32/VB.NTC Trojan
Win32/VB.NVM Trojan
Win32/VB.NWB Trojan
Win32/VB.QPK Trojan
Win32/VB.QTV Trojan
Win32/VB.QTY Trojan
Win32/Spy.Agent.NVL Trojan
Win32/Spy.Agent.OAZ trojan

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 de Sucuri

Sucuri est une entreprise basée en Californie qui intervient dans tout le continent américain. La société a été fondée par deux membres très passionnés par la sécurité des systèmes d'information en mettant l'accent sur deux domaines très distincts : la prévention et la sensibilisation. Créée en 2007, Sucuri a été pensée dès 2004 pour s'attaquer au problème des logiciels malveillants sur le Web.

Pour en savoir plus, veuillez visiter le site Internet : www.sucuri.net

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