



Le ver Win32/Stuxnet vise les systèmes de surveillance industrielle aux États-Unis et en Iran

Contacts Presse

ATHENA Global Services

20 allée Louis Calmanovic
93320 Les Pavillons-sous-bois,
Tel : 01 55 89 08 84
Fax : 01 55 89 08 89
Laëtitia Bonnot
laetitia.b@athena-gs.com

InterPresse

Parc de Garlande
1 rue de l'Égalité
92000 Bagneux
Tel : 01 55 48 05 10
Fax : 01 55 48 05 11
Isabelle Guillou
iguillou@interpresse.fr
Norbert Spitéri
nspiteri@interpresse.fr

A propos d'Athena Global Services

Créée en 1997, ATHENA Global Services est une entreprise indépendante spécialisée dans la distribution de logiciels de sécurité informatique.

A 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

Les Pavillons-sous-Bois, le 20 juillet 2010, ESET, spécialiste de la conception et du développement de logiciels de sécurité, a émis un avertissement contre un ver baptisé Win32/Stuxnet, qui menace les utilisateurs du monde entier en exploitant une vulnérabilité dans Windows Shell®. Cette dangereuse menace a été détectée par ESET et référencée sous l'intitulé LNK / Autostart.A. Le ver est utilisé pour effectuer des attaques ciblées de façon à pénétrer les systèmes SCADA, notamment aux États-Unis et en Iran. SCADA, Supervisory Control And Data Acquisition (télé-surveillance et acquisition de données), sont des systèmes de surveillance utilisés dans de nombreuses industries, par exemple dans l'ingénierie électrique.

Selon ESET Virus Lab, le ver a été actif pendant plusieurs jours, en particulier aux États-Unis et en Iran : près de 58% des infections sont signalées aux États-Unis, 30% en Iran et un peu plus de 4 % en Russie. Les cyber-attaques aux États-Unis ainsi que l'activité accrue du ver en Iran, sont les conséquences de la persistance des tensions entre les deux pays sur les ambitions nucléaires des pays du Moyen-Orient. « *Ce ver est un cas exemplaire d'une attaque ciblée, exploitant une vulnérabilité "zero-day", ou, en d'autres termes, une menace encore inconnue. Cette attaque vise en particulier le système de contrôle industriel SCADA. En bref, ceci est un exemple de malware assisté par ordinateur pour l'espionnage industriel.* », explique Juraj Malcho, chef du laboratoire d'analyse des virus au siège mondial d'ESET à Bratislava, en Slovaquie.

La plupart des dommages causés par le ver sont limités à des objectifs industriels, tandis que les particuliers sont beaucoup moins touchés. « *Jusqu'à présent, le nombre d'ordinateurs infectés est d'une dizaine de milliers, mais il est susceptible d'augmenter* », indique Malcho. Selon l'analyse d'ESET, le ver Stuxnet, ne pose pas plus de problèmes sur les ordinateurs des particuliers que les menaces traditionnelles rencontrées généralement sur les postes de travail. Le danger réside dans la vulnérabilité de l'OS Windows liée aux processus lancés par des fichiers .LNK. Les experts s'attendent à ce que des familles de logiciels encore plus malveillantes commencent à exploiter cette faille de sécurité dans un proche avenir.

La plupart des dommages causés par le ver sont limités à des objectifs industriels, tandis que les particuliers sont beaucoup moins touchés. « *Jusqu'à présent, le nombre d'ordinateurs infectés est d'une dizaine de milliers, mais il est susceptible d'augmenter* », indique Malcho. Selon l'analyse d'ESET, le ver Stuxnet, ne pose pas plus de problèmes sur les ordinateurs des particuliers que les menaces traditionnelles rencontrées généralement sur les postes de travail. Le danger réside dans la vulnérabilité de l'OS Windows liée aux processus lancés par des fichiers .LNK. Les experts s'attendent à ce que des familles de logiciels encore plus malveillantes commencent à exploiter cette faille de sécurité dans un proche avenir.

À propos d'ESET

La société ESET est spécialisée dans la conception et le développement de logiciels de sécurité offrant une protection globale contre les menaces évolutives qui sévissent dans les environnements informatiques. Pionnier en matière de détection proactive des menaces, ESET est aujourd'hui le leader dans ce domaine. ESET a développé un vaste réseau mondial de partenariats, y compris avec des entreprises telles que Canon, Dell et Microsoft. ESET possède des bureaux à Bratislava (Slovaquie), Bristol (Royaume-Unis), Buenos Aires (Argentine), San Diego (USA), Prague (République Tchèque), et est représenté dans plus de 160 pays. Pour plus d'informations, veuillez visiter les sites Internet : www.eset-nod32.fr ou www.athena-gs.com