Trend Micro Threat Research Report :
Trend Micro a neutralisé 9 millions d'attaques ZeuS au cours des 6 derniers mois

Rueil-Malmaison, France – 12 mars 2010 – Trend Micro a récemment constaté une nette progression de la diffusion du virus ZeuS, avec en moyenne 300 échantillons uniques supplémentaires par jour. Ces chiffres sont ceux d'une étude récente qui se penche sur l'organisation criminelle d'Europe de l'Est qui gère ce logiciel malveillant particulièrement dynamique, conçu pour détourner des données bancaires et financières. Trend Micro a ainsi identifié plus de 13 000 échantillons uniques de Zeus sur le seul mois de janvier 2010.

" ZeuS n'est pas nouveau et nous le voyons en action depuis des années. En revanche, la récente recrudescence des attaques est plus inquiétante ", explique Raimund Genes, CTO de Trend Micro. *" ZeuS compte parmi les principales menaces pour la sécurité des internautes et Trend Micro a su y riposter : au cours des 6 derniers mois, nous avons neutralisé 9 millions d'attaques ZeuS et ce chiffre progresse chaque jour. "*

ZeuS en pleine mutation

Trend Micro a également découvert que, sur la majeure partie de l'année dernière, des variantes de ZeuS ont été distribuées via le réseau Avalanche, un botnet à l'origine de campagnes massives de spam. Ces campagnes contrefaisaient plusieurs sites de réseau sociaux populaires et les cybercriminels à l'origine de ces attaques ont également tenté d'imiter des messages email et sites web d'institutions gouvernementales. C'est le cas aux États-Unis pour le Federal Deposit Insurance Corporation (FDIC), le Centers for Disease Control and Prevention (CDC), la Sécurité Sociale américaine ou encore le Trésor Public américain.

Autre évolution importante, les versions les plus récentes de ZeuS disposent désormais d'une nouvelle fonctionnalité : Jabber, un protocole open source de messagerie instantanée. La variante JabberZeuS détourne les identifiants de connexions lors de sessions de connexion à un compte bancaire en ligne. Cette information est relayée en temps-réel via un message instantané au botmaster ZeuS, ce qui permet une connexion immédiate et en parallèle au compte de la victime tout en évitant d'être détecté.

Complémentarité entre ZeuS et BREDOLAB

Selon les recherches menées par Trend Micro, BREDOLAB et ZeuS sont des outils distincts disponibles gratuitement dans le monde souterrain de la cybercriminalité. Leurs fonctions complémentaires expliquent leur présence souvent conjointe. ZeuS se spécialise dans le détournement d'informations à partir des systèmes infectés, tandis que BREDOLAB permet aux cybercriminels de fournir tout type de logiciels à leurs victimes. Lorsqu'une machine est infectée par BREDOLAB, elle reçoit des mises à jour malveillantes régulières, de la même façon qu'elle est mise à jour par un fournisseur d'outil de sécurité.

Une situation économique qui favorise ZeuS

Le succès de ZeuS est notamment dû à la capacité des cybercriminels à recruter des "mules" qui assurent la collecte et le transfert de l'argent détourné, sous couvert d'un emploi à domicile. Avec les conditions économiques actuelles et la recrudescence du

chômage dans de nombreux pays, les cybercriminels parviennent plus facilement à recruter leurs complices. Ces derniers, qui pensent opérer dans le cadre d'un travail, doivent fournir les informations sur leur compte bancaire personnel. Ce dernier est utilisé par les cybercriminels pour réaliser des virements aux complices à partir des comptes bancaires piratés, et pour des montants toujours en deçà des seuils d'alerte des banques. Les complices n'ont plus qu'à re-transférer cet argent vers leurs commanditaires essentiellement basés dans certains pays d'Europe de l'Est.

Quelle protection pour les entreprises ?
Le réseau Botnet ZeuS est conçu pour détourner furtivement les identifiants bancaires et autres données confidentielles. Ce malware se désactive lorsqu'il veut éviter de se faire détecter. Trend Micro offre la technologie et l'expertise adéquates pour neutraliser immédiatement les attaques botnets. Trend Micro™ Smart Protection Network™ fournit une protection instantanée et en temps-réel qui optimise l'ensemble des solutions Trend Micro. Cette infrastructure corrèle des informations provenant de plus de 20 milliards d'emails, de sites Web et de fichiers chaque jour. Les données recueillies sont immédiatement utilisées pour identifier et contrer les menaces les plus récentes.

Les recommandations de Trend Micro

- **Produit Grand public :**
  Trend Micro™ Internet Security
- **Petites entreprises :**
  Worry-Free™ Business Security Standard/Advanced et Services
- **Moyennes et grandes entreprises :**
  OfficeScan™ Client/Server Edition
  Threat Management Services
  InterScan™ Messaging Hosted Security
  InterScan™ Web Security

Pour davantage d'informations, merci de visiter :

http://us.trendmicro.com/us/trendwatch/research-and-analysis/white-papers-and-articles/index.html

À propos de Trend Micro :
Trend Micro Incorporated, acteur majeur de la sécurité des contenus Internet, sécurise les échanges d'informations numériques pour les entreprises et le grand public. Pionnier de ce métier, Trend Micro propose des technologies intégrées pour une gestion unifiée des menaces, qui pérennise l'activité des entreprises, protège les informations personnelles et juguler les logiciels malveillants, le spam, les fuites de données et autres menaces Web. Connectez à Trend Watch surwww.trendmicro.com/go/trendwatch pour en savoir davantage sur ces menaces. Les solutions Trend Micro, disponibles sous différents formats, bénéficient du support en mode 24*7 d'une équipe mondiale d'experts en menaces Web. Nombre de ces solutions sont adossées au Trend Micro Smart Protection Network, une infrastructure de sécurité cloud-client de nouvelle génération qui associe des technologies hébergées de réputation, des feedbacks et l'expertise des chercheurs de TrendLabs, pour ainsi concrétiser une protection en temps-réel contre les menaces Web émergeantes. La société, dont le siège social se situe à Tokyo, est présente à l'échelle mondiale et ses solutions de confiance sont distribuées dans le monde entier via un réseau étendu de partenaires.www.fr.trendmicro.com pour toute information supplémentaire.