Menaces sur les IT : les attaques viennent des US

Les chercheurs du 'lab' Symantec de Cupertino ont fait le constat qu'au deuxième semestre 2006, le tiers des attaques de systèmes informatiques dans le monde provenaient des Etats-Unis, qui demeurent la terre la plus fertile pour toutes les menaces qui pèsent sur nous, via le spam, le phishing et les codes malveillants.

La Chine, de plus en plus pointée du doigt par les autorités américaines comme étant la source de tous les maux qui menacent l'informatique, ne pointe en réalité qu'en seconde place avec 10 % des attaques, suivie par l'Allemagne avec 7 %.

Les Etats-Unis détiennent également, toujours selon Symantec, le triste record des réseaux de 'bots' (zombies). Rappelons qu'un 'bot' est un ordinateur compromis qui est contrôlé à distance par un pirate et inséré dans un réseau de 'bots' exploité comme pompe à spam ou pour d'autres opérations toutes aussi illégales.

Ces réseaux s'appuient sur des serveurs mafieux, ils seraient 4700 selon Symantec, en recul de -25 %, qui alimentent un réseau de 'bots' estimé à 6 millions d'ordinateurs dans le monde, en recul de -25 %. On notera cependant que 26 % des 'bots' seraient en Chine?

En revanche, dans le même temps, le trafic du spam aurait progressé de 5 %, en particulier avec la multiplication des offres financières et d'opérations boursières, jusqu'à atteindre 59 % du trafic total des messageries.

Plus dangereux, Symantec affirme que les Etats-Unis hébergeraient plus de la moitié des '*serveurs d'une économie souterraine*' créée pour organiser des réseaux de transactions clandestines basées sur des données volées.

Un tel réseau permettrait d'exploiter des données confidentielles comme un numéro de carte bancaire ou de sécurité sociale dans les deux heures à deux semaines qui suivent le vol?

Pire encore, ce réseau serait à l'origine d'un commerce mafieux des informations dérobées. Et Symantec de citer des prix, de 1 dollar pour un numéro de carte bancaire à 14 dollars pour une identité complète, nom, date de naissance, sécurité sociale, compte bancaire et carte bancaire !

Dernières remarques, 77 % des attaques ciblent en priorité le navigateur Internet Explorer de Microsoft. Et Symantec anticipe l'émergence d'attaques contre le système d'exploitation Windows Vista. Ainsi que de campagnes de phishing visant les joueurs en ligne et consistant à usurper l'identité des sites de jeux massivement multi-joueurs.

Les conclusions du rapport de Symantec

La principale conclusion du onzième rapport de Symantec sur les menaces Internet est que les cybercriminels utilisent des méthodes d'attaque de plus en plus élaborées, ciblées et malicieuses. Ils s'organisent en réseaux mondiaux pour assurer le développement de leurs activités criminelles.

Toujours motivés par l'appât du gain, ils dérobent ainsi des informations confidentielles sans être repérés.

LE COMMERCE DES DONNEES VOLEES

Pour la première fois dans son rapport, Symantec a étudié le commerce des données et informations confidentielles volées. Elles sont fréquemment mises en vente sur des serveurs commerciaux clandestins. Les pirates informatiques et organisations criminelles utilisent souvent ces serveurs pour vendre des informations dérobées, telles que des numéros de sécurité sociale, de cartes de crédit, d'identification personnelle (PIN), ou des listes d'adresses email.

Au cours du deuxième semestre 2006, 51 % de tous les serveurs commerciaux clandestins se trouvaient aux États-Unis. Les cartes de crédit américaines dotées d'un numéro de contrôle sont vendues sur ce marché clandestin de 14 à 18 dollars, tandis qu'une identité complète (numéro de compte bancaire américain, carte de crédit, date de naissance et numéro d'identification émis par le gouvernement) est vendue de 1 à 20 dollars.

Chevaux de Troie et réseaux bots, qui ont augmenté au cours de la période étudiée, mettent en danger les données confidentielles stockées sur un ordinateur infecté. Ils peuvent conduire à d'importantes pertes financières, en particulier s'il s'agit de numéros de cartes de crédit ou d'informations bancaires. Les menaces visant les informations confidentielles représentent 66 % des 50 principaux codes malicieux répertoriés par Symantec, soit 48 % de plus qu'au premier semestre 2006. Les menaces permettant d'exporter des données utilisateur, (noms d'utilisateur ou des mots de passe), représentent 62 % des menaces visant les informations confidentielles, soit 38 % de plus qu'au premier semestre.

VOLS D'IDENTITE ET FUITES DE DONNEES

Les informations confidentielles exploitées pour le vol d'identité sont souvent dérobées lors de fuites de données. Symantec a analysé les fuites de données provoquées par les pirates, le vol ou la perte de matériel informatique et les défaillances des règles de sécurité. Les fuites de données et l'éventuelle utilisation d'informations confidentielles pour le vol d'identité peuvent par exemple faire perdre à une entreprise la confiance de ses clients, la rendre responsable devant la loi ou causer des litiges coûteux. Dans 25 % des cas, les fuites de données ont touché le secteur gouvernemental.

LE PHISHING SE CALQUE SUR LA SEMAINE DE TRAVAIL POUR MIEUX IMITER LES EMAILS D'ENTREPRISES

Au cours du deuxième semestre 2006, Symantec a également répertorié un total de 166.248 messages de phishing uniques, soit une moyenne de 904 par jour, ce qui correspond à une progression de 6 % par rapport au premier semestre. Pour la première fois, Symantec analyse la corrélation entre le jour de la semaine ou les événements saisonniers et les attaques de phishing. Sur l'ensemble de l'année 2006, Symantec a détecté en moyenne 27 % de messages de phishing en moins les week-ends, pour une moyenne de 961 messages de phishing par jour pendant le reste de la semaine. Cette tendance indique que l'activité de phishing est plus ou moins calquée sur la semaine de travail et que les attaquants essaient d'imiter les courriers électroniques émis par les entreprises officielles. Toutefois, ces chiffres peuvent également souligner le caractère éphémère

des campagnes de phishing, celles-ci étant plus efficaces lorsque les victimes les lisent rapidement après leur diffusion. Symantec a constaté une augmentation du phishing pendant les principales périodes de congé ou lors de grands événements comme la coupe du monde de la FIFA, par exemple. En effet, les attaquants ont peut-être moins de difficulté à élaborer des attaques de social engineering sur des thèmes tournant autour de ce type d'événement.

SPAM ET FRAUDES EN LIGNE : DES MENACES TOUJOURS PLUS SOPHISTIQUEES

Symantec a observé une grande quantité d'attaques coordonnées combinant spam, code malicieux et fraude en ligne. À noter que 30 % du spam touchant le marché des services financiers sont générés par le développement du spam » pump-and-dump » (escroqueries boursières). Dans une campagne de « pump and dump » (littéralement, gonfler et jeter), les cybercriminels achètent des actions à bas prix puis « gonflent » artificiellement leur valeur en diffusant des spams contenant de fausses prévisions sur la future haute performance de ces actions. Les destinataires du spam se fient à ces prévisions, achètent l'action en question et génèrent donc une demande qui fait monter le prix. Lorsque le prix est suffisamment haut, les cybercriminels vendent leurs actions et font donc des bénéfices.

CHEVAUX DE TROIE ET VULNERABILITES ZERO DAY EN TRES FORTE AUGMENTATION

Sur la seule période du deuxième semestre 2006, Symantec a répertorié dans le monde plus de six millions de bots – des ordinateurs « zombies » qui répondent aux commandes à distance d'un attaquant – soit 29 % de plus par rapport au premier semestre. En revanche, si le nombre d'ordinateurs infectés est en augmentation, Symantec a constaté une diminution de 25 % du nombre de serveurs contrôlant ces réseaux de PC zombies. Cette baisse est, peut être, le résultat des efforts déployés pour éliminer ces serveurs, poussant ainsi les propriétaires à regrouper leurs réseaux de bots et à en augmenter la taille.

De plus, l'augmentation considérable du nombre de chevaux de Troie pendant le deuxième semestre 2006 confirme les prévisions de Symantec qui annonçait dans son précédent rapport que les attaquants semblaient abandonner les vers d'envoi en masse par courriers électroniques au profit des chevaux de Troie. Les chevaux de Troie représentent ainsi 45 % des 50 principaux codes malicieux, soit une progression de 23 % par rapport au premier semestre 2006.

Symantec révèle également une augmentation spectaculaire du nombre de vulnérabilités 'zero-day' inconnues, ce qui signifie que les particuliers et les entreprises sont exposés à davantage de menaces inconnues. Les vulnérabilités » zero-day » n'étant découvertes qu'au moment où elles sont exploitées, elles sont devenues un outil de choix pour les attaques ciblées qui contaminent les victimes à l'aide d'un code malicieux. Au cours du deuxième semestre 2006, Symantec a répertorié 12 vulnérabilités 'zero-day', contre une seule au cours du premier semestre.

Ces vulnérabilités sont découvertes par des pirates, ou bien achetées sur le marché noir. Elles sont ensuite utilisées pour exploiter des systèmes et y installer un code malicieux, des logiciels publicitaires ou des applications trompeuses.

Pour la première fois, Symantec a étudié dans son rapport les pays qui génèrent le plus d'activités malicieuses (bots, serveurs de commande-contrôle de bots, sites de phishing, codes malicieux, hôtes relais de spam et attaques Internet). Pour le deuxième semestre 2006, la palme des activités malicieuses revient aux États-Unis,

avec 31 % du total mondial. Quant à la Chine, elle comptabilise le plus grand nombre d'ordinateurs zombies, avec 26 % du total mondial.