Les infrastructures sensibles ont deux fois plus de risque d'être la cible des cybercriminels

Le premier fournisseur mondial de sécurité Web en mode SaaS présente son rapport mondial annuel sur les menaces

Paris, le 15 février 2010 — ScanSafe, pionnier et leader de la sécurité Web en mode SaaS, publie ce jour son rapport mondial annuel sur les menaces qui révèle que les infrastructures sensibles comme celles dans l'énergie, le secteur pharmaceutique ou le secteur public ont deux fois plus de risque d'être la cible des cybercriminels que d'autres organisations. Ce rapport se base sur l'analyse de plus de mille milliards de requêtes Web traitées en 2009 par le Threat Center de ScanSafe pour le compte d'entreprises clientes réparties dans plus de 100 pays. Il constitue la plus importante analyse de sécurité du trafic en temps réel.

Les recherches de ScanSafe mettent en lumière une tendance inquiétante – les organisations qui manipulent les données intellectuelles les plus précieuses rencontrent des malware Web à une fréquence bien plus élevée que les autres secteurs. Selon le rapport, les secteurs les plus exposés sont :

Secteur énergie & pétrole: un taux d'exposition directe à des chevaux de Troie visant le vol de données supérieur de 356% par rapport aux autres secteurs
Secteur pharmaceutique et chimie: taux supérieur de 322%
Administration publique: taux supérieur de 252%
Secteur banque & finance: taux supérieur de 204%

"*L'idée selon laquelle les cybercriminels ne cherchent qu'à voler des données utiles à la fraude à la carte de crédit et au vol d'identité est erronée. Dans les faits, les cybercriminels déploient un filet bien plus vaste*," explique Mary Landesman, Chercheur Senior en sécurité chez ScanSafe. "*Les coordonnées de cartes de crédit des particuliers ne sont pas grand chose par rapport à la valeur des données d'infrastructure et intellectuelles de ces secteurs sensibles. Le message est clair : la cyber-guerre est déjà entamée. Le Web constitue le champ de bataille et l'entreprise se situe en ligne de front.*"

Par ailleurs, le rapport révèle que les malware véhiculés par le Web ont plus que doublé au cours de l'année écoulée. Début 2009, l'entreprise moyenne connaissait 8 rencontres avec des malware Web par jour. A fin 2009, le taux d'exposition avait plus que doublé avec 19 rencontres par jour. Sur l'ensemble de ces rencontres, 23% concernaient des malware 'zero-day' impossibles à détecter par des méthodologies à base de signatures, 19% concernaient des rencontres directes avec des chevaux de Troie visant le vol de données.

Parmi les autres conclusions majeures, il faut noter:

Les malware sont les outils de prédilection d'une nouvelle économie Internet parallèle
La structure économique derrière le cybercrime actuel n'est pas sans ressembler à la structure économique de toute autre activité mondiale. Les attaquants tiennent plusieurs rôles dans cet univers commercial, parmi lesquels « le propriétaire unique », « l'homme du milieu », « le développeur » et « l'acheteur ».

Le botnet Gumblar a occupé le devant de la scène en 2009
14% du nombre total de malware Web bloqués sur l'année émanaient de Gumblar. Novembre 2009 a connu un pic montant à 35% de tous ces malware bloqués. Asprox se positionne en deuxième position avec 2% de tous les malware bloqués et Zeus en troisième position avec 1% de tous les malware bloqués.

Fichiers PDF malveillants à la hausse, fichiers Flash malveillants à la baisse
Les fichiers PDF malveillants ont constitué 56% des exploits rencontrés sur le Web au premier trimestre 2009 et ont atteint 80% au dernier trimestre. Les exploits Flash rencontrés sur le Web ont

connu une baisse et sont passés de 40% au premier trimestre 2009 à 18% au dernier trimestre. Cette tendance indique sans doute la préférence des attaquants pour les exploits PDF, sûrement liée à la disponibilité croissante de vulnérabilités et à l'usage et l'adoption des fichiers PDF qui se répandent de plus en plus sur le lieu de travail.

"*Pour faire face aux défis des années à venir, il faut ajuster notre vision des choses à la nouvelle réalité. Il faut dépasser ce que nous connaissons et envisager les enjeux qui sont déjà d'actualité : une activité criminelle de récupération de données,"* commente Mary Landesman. "*Nos moyens de défense doivent aller au-delà des limites du brick-and-mortar jusque dans le nuage, pour garantir une protection finale des personnes et des actifs les plus sensibles, ce quel que soit le système d'exploitation, l'équipement ou l'emplacement géographique."*

Pour vous procurer un exemplaire intégral du rapport mondial annuel sur les menaces de Scansafe, merci de vous rendre surhttp://www.scansafe.com/fr

A propos de ScanSafe
ScanSafe, (http://www.scansafe.com/fr) qui fait maintenant partie de Cisco, est le pionnier et le premier fournisseur mondial de Sécurité Web en mode SaaS garantissant aux entreprises un environnement Internet sûr et productif. Les solutions ScanSafe gardent les malware hors des réseaux d'entreprises et permettent à ces dernières de contrôler et de sécuriser l'utilisation du Web. En tant que solution SaaS, ScanSafe élimine les coûts d'investissement et l'administration d'infrastructures en interne, réduisant de manière significative le coût total d'acquisition. Grâce à sa technologie proactive et multicouche de détection des menaces, Outbreak Intelligence ™, ScanSafe traite plus de 20 milliards de requêtes Web et bloque 200 millions de menaces chaque mois pour des clients répartis dans plus de 100 pays.

En 2009, l'entreprise a reçu la récompense "Best Content Security" solution par SC Magazine Europe pour la troisième année consécutive.