

Les vulnérabilités et menaces informatiques atteignent un niveau record depuis 2000 **Sécurité**

Posté par : JPilo

Publié le : 20/1/2014 13:00:00

Les sites sectoriels et commerciaux comptent parmi les trois premières catégories où se visent les programmes malveillants. **Le Rapport Annuel sur la Sécurité 2014 de Cisco**, révèle que le nombre total de vulnérabilités et de menaces a atteint un niveau record depuis le début de leur recensement en mai 2000.

En octobre 2013, le nombre total d'alertes cumulées a augmenté de 14 % en glissement annuel par rapport à 2012.

Les conclusions du rapport offrent un tableau saisissant de l'évolution rapide des enjeux de sécurité auxquels sont confrontés les entreprises, les départements informatiques, et les particuliers.

Les méthodes employées par les cyber-criminels sont multiples :

Ingénierie sociale visant à dérober les mots de passe et identifiants d'utilisateurs, infiltrations « hide-in-plain-sight » (si évidentes qu'elles passent inaperçues), ou encore l'exploitation de la confiance que les internautes accordent nécessairement lorsqu'ils effectuent des transactions financières, utilisent les services publics, ou échangent sur les réseaux sociaux.



Principales conclusions du rapport :

Une pénurie de spécialistes de la sécurité informatique à prévoir en 2014

Le rapport souligne que **l'année 2014** sera marquée par une pénurie de plus d'un million de professionnels spécialisés dans le domaine de la sécurité, ce qui pourrait mettre à mal les capacités des entreprises à contrôler et sécuriser les réseaux.

Du fait de leur sophistication, les technologies et tactiques employées par les criminels en ligne et leurs tentatives incessantes d'infiltration dans les réseaux et de vol de données ont désormais pris de vitesse les professionnels de l'informatique et de la sécurité.

La plupart des entreprises ne bénéficient pas de personnel ou de systèmes dédiés en permanence à la surveillance des réseaux étendus et à la détection des menaces. Pourtant, ces investissements sont les seuls capables d'appliquer des mesures de protection efficaces en temps voulu.

â€¢ 99% des malwares mobiles ont ciblé les appareils Android en 2013

Avec 43,8 % des occurrences recensées, Andr/Qdplugin-A représente le logiciel malveillant le plus fréquemment détecté. Le malware transite habituellement via des versions dupliquées d'applications légitimes distribuées par des plateformes commerciales non-officielles.

â€¢ Les industries chimiques et pharmaceutiques, ainsi que le secteur de la fabrication électronique, principales victimes des infections malveillantes.

En 2012 et en 2013, les malwares ont connu une recrudescence notable au sein des secteurs de l'agriculture et de l'exploitation minière, auparavant considérés comme des industries à faible risque. Les occurrences de malwares continuent de croître dans les secteurs de l'énergie ainsi que dans les industries gazière et pétrolière.

â€¢ Les grandes entreprises, passerelles vers les sites web piratés

L'étude d'un échantillon de 30 entreprises issues du classement Fortune 500 a révélé que 100 % des réseaux de ces entreprises avaient généré un trafic visiteurs vers des pages Web hébergeant des logiciels malveillants. En effet, 96% des réseaux étudiés ont dirigé du trafic vers des serveurs piratés, alors que 92 % d'entre eux ont généré du trafic vers des pages vierges, qui hébergent généralement des activités malveillantes.

â€¢ La recrudescence et le renforcement des attaques DDoS (par déni de service)

Les attaques DDoS (par déni de service) perturbent le trafic depuis et en direction de sites Internet ciblés, et sont capables de paralyser les FAI. Elles ont progressé à la fois en termes de volume et de gravité. Certaines attaques DDoS ont pour objectif de dissimuler d'autres activités néfastes, telles que des fraudes électroniques perpétrées avant, pendant ou après une campagne DDoS, volontairement destabilisantes et retentissantes.

â€¢ Les chevaux de Troie multi-cibles constituent les attaques malveillantes les plus fréquemment repérées sur le Web

Les attaques des chevaux de Troie multi-cibles représentent 27 % de l'ensemble des attaques enregistrées en 2013. Les scripts malicieux, notamment les exploits ou les iframes malveillants, constituent la deuxième catégorie d'attaques la plus courante, avec 23 %. Les chevaux de Troie destinés au vol de données, tels que les password stealers et portes dérobées, représentent quant à eux 22 % des actes malveillants recensés sur la toile.

Le déclin régulier du nombre d'adresses IP et d'hébergeurs de malwares uniques qui a chuté de 30 % entre janvier et septembre 2013 laisse penser que les activités malveillantes se concentrent désormais sur un nombre plus restreint d'adresses IP et d'hébergeurs.

â€¢ Java demeure le langage de programmation le plus fréquemment visé par les cybercriminels.

D'après les données fournies par Sourcefire, société désormais détenue par Cisco, les exploits Java constituent la vaste majorité (91 %) des corruptions recensées par les indicateurs IOC (Indicators Of Compromise).

Tendances majeures de la cybercriminalité :

â€¢ Une expansion et une sophistication croissantes de l'univers des menaces. Les simples attaques aux conséquences limitées ont été remplacées par des opérations de cybercriminalité minutieusement orchestrées et financées, capables d'occasionner des dommages économiques considérables et d'affecter la réputation de leurs victimes, qu'elles appartiennent au secteur privé ou à la sphère publique.

â€¢ La complexité accrue des menaces et des technologies, qui résulte de l'adoption de plus en plus massive des Smartphones et du Cloud, permet d'étendre le champ d'attaques comme jamais auparavant. Les nouvelles catégories d'appareils et les architectures d'infrastructure les plus innovantes offrent aux pirates la possibilité d'exploiter des faiblesses jusqu'alors insoupçonnées et de s'attaquer à des composants mal protégés.

â€¢ Les cyber-criminels ont conscience qu'il est nettement plus rentable d'exploiter la puissance de l'infrastructure d'Internet que de simplement infiltrer les appareils et ordinateurs de particuliers. Ces attaques à l'échelle de l'infrastructure ciblent des serveurs d'hébergement en ligne bénéficiant d'un positionnement stratégique, des serveurs de nom de domaine ou des DataCenters.

Leur objectif est de multiplier les attaques sur les très nombreux systèmes individuels hébergés par ces serveurs. En ciblant l'infrastructure Internet, les pirates ébranlent la confiance des utilisateurs dans les terminaux qui y sont connectés ou qui y ont accès.