Communiqué de presse

Fortinet présente les menaces et virus les plus répandues sur Internet pour le mois d'Aout.

Paris, le 31 Août 2009 - Fortinet®, pionnier et fournisseur de solutions de sécurité réseau et de systèmes unifiés de sécurité UTM (Unified Threat Management), présente son rapport des menaces les plus répandues sur Internet au mois d'Août.

Si la période des vacances touche bientôt à sa fin, force est de constater qu'il n'y a pas eu de trêve des menaces sur Internet pendant l'été. Comme l'indique Fortinet, la période estivale a donné lieu à une recrudescence d'activité malveillante, notamment sous l'effet de multiples campagnes de spams. En outre, une hausse sensible des vulnérabilités logicielles a été observée, du fait d'*exploits** « in-the-wild », c'est-à-dire en libre circulation. Parmi les faits marquants de ce rapport, on peut notamment mentionner les suivants :

- **ZBot** et ses variantes volent la vedette aux *worms*** qui, ces dernières années, avaient marqué le paysage des menaces Internet. Le 24 juillet dernier, plusieurs variantes de Zbot ont inondé le cyber-espace et dépassé des niveaux record d'activité. Une de ces variantes était diffusée via HTML/Agent.E, une pièce jointe aux e-mails exploitant le piège bien connu de l'eCard pour dérober puis revendre les données personnelles des internautes. Une nouvelle variante a fait entrer ZBot dans le Top 10 des menaces les plus répandues le mois dernier sans toutefois détrôner le cheval de Troie W32/OnlineGames.BBR, visant les jeux en ligne, qui reste en tête du classement pour le troisième mois consécutif.

*Programme informatique permettant d'exploiter une faille de sécurité

** Programme informatique permettant d'exploiter une faille de sécurité

- **Des spams qui continuent de leurrer les internautes les moins incrédules :** si la célèbre campagne eCard d'ingénierie sociale a poursuivi son œuvre en profitant des internautes non méfiants, le rapport de ce mois-ci souligne l'apparition d'un procédé

de transfert d'argent frauduleux (« money mule ») qui, bien que novateur dans sa forme, n'en demeure pas moins un grand classique. Au moyen d'une fausse annonce d'emploi, l'arnaque exploite le nom d'une entreprise connue ainsi que le désespoir des victimes. Objectif : leur faire miroiter un gain facile et rapide dans le cadre d'une opération de blanchiment d'argent. Israël fait son entrée dans la liste des cinq pays à recevoir le plus grand nombre de spams, tandis que les États-Unis, le Japon et la France se partagent le volume restant de spams détectés.

- **Motifs de préoccupation au sujet de l'exécution de code à distance :** soulignant une tendance continue à la hausse du nombre de vulnérabilités logicielles, les niveaux de menaces observés en août ont augmenté de manière significative par rapport à juillet. Parmi les 168 nouvelles vulnérabilités détectées, 62 sont apparues comme étant activement exploitées « in the wild », et une part importante de ces vulnérabilités ont été jugées critiques. Une vulnérabilité dite « critique » indique généralement une préoccupation quant à l'exécution de code à distance – un moyen simple pour les criminels d'infiltrer un système. Deux vulnérabilités en libre circulation sur Microsoft Office Web Components (MS09-043) et sur Adobe Reader/Flash (APSA09-03) ont également été détectées comme ayant eu une activité continue d'exploitation durant cette période.

« *Les actes malveillants observés ce mois-ci se sont inspirés de plusieurs procédés bien connus mais avec de nouveaux pièges à la clé, ce qui prouve bien que les cyber-criminels ont encore plus d'une corde à leur arc et, à l'évidence, n'ont pas fait de pause pendant la période des vacances estivales* », explique Guillaume Lovet, responsable de l'équipe anti menaces EMEA chez Fortinet. « *Dans un contexte où les criminels espèrent pouvoir duper le grand public en reprenant leurs bonnes vieilles recettes quasiment à l'identique, on ne peut assez souligner la nécessité de savoir en qui et en quoi nous pouvons avoir confiance – un élément qu'il est essentiel de prendre en compte pour développer un modèle de sécurité solide.* »
Pour consulter le rapport d'Août dans son intégralité, veuillez vous rendre sur le site FortiGuard de Fortinet : http://www.fortiguard.com/report/roundup_august_2009.html.
Pour être informé(e) en continu des nouvelles menaces identifiées par Fortinet, vous pouvez ajouter à vos favoris le site Internet du FortiGuard Center (http://www.fortiguardcenter.com/) ou encore lier la page suivante à votre flux RSS : http://www.fortinet.com/FortiGuardCenter/rss/index.html. Pour en savoir plus sur l'analyse

des menaces ou les technologies de sécurité disponibles, vous pouvez également vous rendre sur le blog de Fortinet : http://blog.fortinet.com.

Enfinm, pour en savoir plus sur les services d'abonnement FortiGuard, veuillez vous rendre à l'adresse suivante : http://www.fortinet.com/products/fortiguard.html.

À propos de Fortinet

Fortinet est un des principaux fournisseurs de solutions de sécurité réseau et le leader des systèmes unifiés de sécurité Unified Threat Management ou UTM. Les solutions Fortinet constituent la nouvelle génération des systèmes de protection de réseau en temps réel et ont été conçues pour intégrer plusieurs niveaux de sécurité – incluant les fonctions pare-feu, antivirus, antispam, VPN, filtrage de contenu, et prévention des intrusions et spyware– permettant à ses clients de détecter et de contrer en temps réel les attaques faites au niveau du réseau et du contenu. Basées sur la technologie ASIC et sur une interface unifiée, les solutions Fortinet offrent des fonctionnalités avancées en matière de sécurité, qui s'étendent de l'utilisateur nomade aux installations basées sur châssis intégrant gestion et reporting.

Les solutions Fortinet ont reçu de nombreuses récompenses à travers le monde et sont les seuls produits de sécurité à détenir cinq certifications ICSA Labs (pare-feu, antivirus, IPSec VPN, IPS réseau et antispam). Fortinet est basée à Sunnyvale en Californie.

###