Communiqué de presse

Fortinet enregistre en octobre la plus forte activité de malware depuis le début de l'année

Montée en puissance des scarewares sous forme de logiciels de sécurité factices

Paris, le 13 Novembre 2009 – Fortinet®, l'un des principaux acteurs du marché de la sécurité réseau et leader mondial des solutions UTM (gestion unifiée des menaces), présente son dernier rapport des menaces les plus répandues sur Internet au mois d'octobre. Ce rapport indique un niveau très élevé d'activité de malware – quatre fois plus élevé qu'en septembre et la plus forte activité depuis plus de douze mois. Dans le sillage des tendances observées en septembre, les attaques de *scareware* ont affiché ce mois-ci un niveau record, tant par leur nombre que par les préjudices causés. Au total, les sept variantes de malware figurant au top 10 des menaces les plus répandues pointent toutes vers des *scarewares* – un résultat qui atteste de la rapidité, de la puissance et de la récurrence de ces attaques. Ces mauvaises nouvelles viennent s'ajouter à d'autres campagnes de *scareware* sous forme de botnets (réseaux d'ordinateurs zombies), de publicités corrompues et d'attaques types Optimisation de Moteur de Recherche (SEO).

Voici les principaux enseignements à tirer du dernier rapport Fortinet des menaces les plus répandues sur Internet :

- **Les scarewares célèbrent Halloween mais cachent leurs intentions malveillantes –** Contribuant de manière significative à la hausse d'activité malveillante depuis septembre, les scarewares dominent à nouveau le paysage des menaces Internet en se faisant passer pour de faux logiciels de sécurité, sous le nom d'AntiVirus Pro 2010. Les internautes sont incités à acheter le logiciel pour résoudre leurs prétendus problèmes de sécurité et, ce faisant, s'exposent à des conséquences graves : des téléchargeurs se mettent en contact avec un serveur distant pour déployer sur l'ordinateur de l'internaute un dispositif de chargement malveillant et transmettre au serveur les données mises à jour par la victime. D'autres composants

peuvent être associés aux scarewares – comme des agents-robots (bots) ou des logiciels malveillants qui prennent en otage les données personnelles (ransomware). Une fois le système infecté, les vannes sont ouvertes et les cybercriminels ont toute latitude pour perpétrer leurs actes. L'activité de scareware a été telle au mois d'octobre que les virus Virut et Netsky sont sortis du top 10 pour la première fois en un an.

- **Les botnets en progression –** En octobre, le cheval de Troie téléchargeur Bredolab s'est combiné à plusieurs téléchargeurs de scareware pour créer une nouvelle « surprise ». Suivant un mode opératoire comparable à celui des scarewares, Bredolab contacte son réseau pour obtenir les derniers composants à télécharger, au premier rang desquels – ce mois-ci – les installateurs d'AntiVirus Pro 2010. Via cette chaîne de téléchargement, Bredolab est également en lien avec le célèbre *keylogger* Zbot et crée ainsi un dispositif couplant un cheval de Troie dangereux et avide de données à un scareware foncièrement nocif – un mélange de menaces détonnant, chaque menace étant reliée à différents sites de contrôle. Les deux principales variantes de Bredolab détectées ce mois-ci étaient W32/Bredo.G et W32/Bredolab.X. Elles ont notamment été identifiées lors de campagnes de spam utilisant de fausses factures DHL.

- **Les affiliés étendent la portée des scareware –** S'il ne fait aucun doute que les scarewares sortent ce mois-ci en tête du classement des menaces les plus répandues sur Internet, leurs niveaux élevés d'activité sont en partie imputables aux célèbres et lucratifs programmes d'affiliés qui offrent à leurs participants une somme d'argent intéressante pour chaque logiciel téléchargé et acheté. Des outils et des kits directement opérationnels sont proposés aux affiliés participants, accélérant d'autant la diffusion des scarewares et d'autres composants malveillants.

« *Les volumes élevés de scareware observés en septembre se sont consolidés en octobre pour atteindre des niveaux records. Ces menaces s'avèrent d'autant plus dangereuses que les modes de diffusion ne cessent d'évoluer et que les combinaisons d'attaques ajoutent en complexité », souligne Guillaume Lovet, responsable de l'équipe de recherches sur les menaces et la sécurité Internet chez Fortinet. « La constance à laquelle ces menaces se répètent montre que les vieux schémas continuent d'offrir aux cybercriminels des 'solutions'*

efficaces. Entreprises et consommateurs doivent prendre leurs responsabilités et se donner les moyens de mieux appréhender ces menaces en se dotant d'une solution de sécurité multi-niveaux, à même de s'adapter aux caractéristiques – aussi variées que changeantes – des activités malveillantes, qu'il s'agisse de tentatives ou de véritables attaques. »

Pour consulter le rapport d'Octobre dans son intégralité, veuillez vous rendre sur le site FortiGuard de Fortinet : http://www.fortiguard.com/report/roundup_october_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. D'autres discussions sur les technologies de sécurité and analyses des menaces cybercriminelles sont disponibles sur le blog de FortiGuard : http://blog.fortinet.com. Enfin, 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.

###