



**Dossier de Presse
2008**

La cybercriminalité

Historique du groupe Fortinet

Créé en 2000 par Ken Xie, véritable précurseur et ancien CEO fondateur de NetScreen Technologies (devenu Juniper), Fortinet est reconnu comme étant **pionnier et leader du marché de l'UTM** (Unified Threat Management). L'appellation UTM désigne les solutions de protection globale face aux menaces Internet, proposées sous la forme de boîtiers de sécurité multifonctions.

Installée à Sunnyvale en Californie, l'entreprise est également présente sur le continent américain au Canada et au Mexique, ainsi que dans la plupart des pays d'Europe, en Asie en Afrique et au Moyen-Orient. En Europe, le support technique et le centre de formation Fortinet sont basés en France, à Sophia Antipolis. L'équipe commerciale française est installée à Paris-La Défense.

Chiffre d'affaires année fiscale 2005	\$100M+
Effectif Monde	1000 +
Effectif France	10

Le positionnement de Fortinet : la protection complète, en temps réel

Les entreprises subissent un nombre grandissant d'attaques réseau axées sur les contenus telles que virus, vers et chevaux de Troie véhiculés par des activités apparemment inoffensives comme la navigation sur Internet ou la communication par email.

Contrairement aux systèmes de protection classiques qui protègent de manière passive les informations des entreprises, Fortinet fournit une protection en temps réel qui possède l'avantage de ne pas ralentir la navigation sur Internet.

Cette protection globale prévient les attaques d'internautes malveillants et des logiciels automatiques bombardant les boîtes email de spams (publicité par email non réclamée). Protéger son entreprise avec l'un des boîtiers Fortinet revient à sécuriser non seulement les informations parfois confidentielles mais également le réseau informatique de l'entreprise.

Les points clef du positionnement de l'offre Fortinet sont des systèmes de sécurité intégrés, fournissant une gamme complète de fonctions de sécurité (anti-virus, pare-feu, anti-spam, filtrage web, prévention des intrusions, etc) au sein d'une même plate-forme ; une gestion centralisée de ces plate-formes de sécurité ; un mode de

licence par boîtier et non par utilisateurs, rendant la solution déployée beaucoup moins coûteuse.

Fortinet propose une gamme complète de boîtiers de sécurité multi-menaces qui s'adresse à tous les types d'entreprises. Fortinet compte ainsi plus de 20 000 clients à travers le monde, dont des grands groupes industriels, des opérateurs télécom et de nombreux gouvernements, En France, Fortinet travaille avec des entreprises de premier plan telles que LVMH, Orange Business Services, Canal +, Interpol, Cap Gemini et de nombreux ministères.



Guillaume Lovet, expert en cybercriminalité !



Depuis mars 2004, Guillaume Lovet est responsable de l'équipe 'anti-menaces' pour la région EMEA chez Fortinet.

Impliqué dans des activités de recherche dans le domaine de l'anti-virus, membre de l'AVIEN (Anti-virus Information Exchange Network) et intervenant régulier dans des conférences de renommée internationale telles que AVAR, EICAR et VB, Guillaume est aujourd'hui un expert reconnu du monde de l'anti-virus.

Avant de rejoindre Fortinet, Guillaume a travaillé pour la société suisse Visiowave (aujourd'hui division de General Electrics) en tant que développeur C++ au sein du groupe sécurité de l'entreprise et pour TPS où il fut en charge de réaliser une étude sur la sécurité et les données cryptographiques appliquées à la télévision numérique. Guillaume est titulaire d'un Master's Degree en Electrical and Computer Engineering de l'université Georgia Tech aux Etats-Unis.

Guillaume a rédigé plusieurs études révélant les informations données ci-dessous. Il intervient sur **tous les sujets liés à la cybercriminalité** ou cyberdélinquance :

- **le spamming,**
- **le phishing,**
- **le carding,**
- **le herding,**
- **le cyber-racket,**
- **l'espionnage industriel**
- **les profils des cybercriminels ; leur organisation**

La cybercriminalité dépassera-t-elle la criminalité traditionnelle ?

105 milliards de Dollars. C'est le gain annuel de la cybercriminalité aux Etats-Unis en 2006 d'après des experts du gouvernement Fédéral américain. Cette recette annuelle dépasserait celle du trafic de drogue. Un constat alarmant qui révèle la montée en puissance des hackers et autres pirates de l'Internet. Mais qui sont ces nouveaux criminels ? Quel est leur but ? Et, qui est menacé ?

Les hackers sont partout. Ils sont nombreux, inventifs et très organisés. A l'instar de la criminalité traditionnelle, les cybercriminels se répartissent en diverses classes. Les plus jeunes, âgés de 20 ans maximum, sont la force ouvrière du piratage. Maîtrisant les opérations courantes et parfois rébarbatives de piratage, ils vendent des listes de cartes de crédit accompagnées de leur code ou des listes d'adresses e-mail permettant l'envoi de spams. Ensuite, viennent les professionnels ou autodidactes en programmation informatique qui créent et vendent des logiciels permettant de pirater des ordinateurs. D'autres s'occupent de transformer les fonds disponibles sur des comptes en banque piratés, en argent utilisable. Enfin, l'implication de la mafia dans la cybercriminalité ne peut être écartée. Même s'il est difficile de prouver son implication, de tels revenus ne doivent pas laisser insensibles les barons du crime.

Si les hackers ont en commun un esprit mathématique et une connaissance étendue des outils de surveillance de l'Internet, ils n'ont pas les mêmes ambitions.

La gloire, le « fun », ou le goût du risque étaient, encore récemment, les motivations des pirates. Ils recherchent désormais un salaire. Certains n'ont que cette activité pour gagner leur vie. Si un pirate, il y a une dizaine d'années, forçait le serveur de Microsoft pour prouver sa valeur et décrocher un stage, le même court aujourd'hui après un revenu régulier.

Le point marquant de ces dernières années est l'ébauche d'une hiérarchie parmi les hackers. Les plus jeunes peuvent espérer gagner quelques centaines de dollars par mois, les programmeurs quelques milliers et certains génies du Web

remplissent des missions leur rapportant plusieurs dizaines de milliers de Dollars. Ces derniers sont à la tête de la pyramide.

Pour ces cadors du Net, deux types de missions peuvent être mis en lumière. **Le premier est l'extorsion.** Un pirate va contacter une entreprise qui réalise son chiffre d'affaire sur Internet et la menacer de bloquer l'accès au site, si une somme d'environ \$10 000 ne lui est versée. En cas de refus, le pirate se fera une joie de joindre la parole aux actes et empêchera l'accès des internautes au site. Une fois le site réparé, le pirate envoie un deuxième mail où il demandera cette fois \$40 000 pour les épargner pendant une année sous peine d'une autre journée de chômage technique. Le chiffre d'affaire d'une journée dépassant souvent cette rançon, le site va céder. De telles pratiques sont courantes. Mais seule une faible proportion est communiquée par les entreprises, qui ne veulent pas ébruiter un tel chantage.

Le second est lié à l'espionnage industriel. Né avec l'industrie, il a évolué avec les nouveaux moyens de communication. Une société prend contact avec un pirate chevronné. Il sera chargé de récupérer des informations confidentielles. Brevets, fichiers clients... La cible est la propriété intellectuelle.

De telles missions rapportent au pirate quelques dizaines de milliers de dollars.

Ainsi, cette société de l'ombre de plus en plus organisée, vit de l'argent circulant sur Internet. Mais qui est réellement concerné ?

Malheureusement, tout le monde. Du quidam qui vérifie son compte en banque, aux banques elles-mêmes, personne n'est à l'abri. Outre les actes criminels de haut vol qui attaquent les entreprises, le phishing est l'une des activités les plus dangereuses. C'est une technique qui vise les particuliers. Chacun peut recevoir dans sa boîte email, un courrier provenant de sa banque. En l'ouvrant, le message propose un lien vers le site de la banque. L'internaute clique donc sur le lien et arrive, sans le savoir, sur un site fantôme. Ressemblant parfaitement au site officiel, cette page pourra récupérer mot de passe et numéros de comptes de l'utilisateur candide. Cette technique peut être employée à la chaîne et ainsi piéger des dizaines de personnes. L'argent présent sur le compte est maintenant disponible. Le pirate utilisera un intermédiaire pour retirer l'argent, limitant ainsi son exposition.

In fine, empêcher le piratage n'est pas chose aisée. L'infiltration par la police d'Internet des réseaux de pirates est une idée. Cependant, pour atteindre les « gros poissons », ces enquêteurs infiltrés doivent remplir certaines missions illégales. Dilemme : faut-il commettre ces actes illégaux pour démanteler un potentiel réseau ou ne pas s'immiscer dans ces combines et renforcer la surveillance ? En ce qui concerne les particuliers, la solution la plus efficace semble être encore informer et éduquer sur les techniques cybercriminels les plus répandues. Ainsi prévenus, les utilisateurs ne tomberont pas dans les pièges parfois flagrants des hackers.

L'équipe de Fortinet

VP EMEA	Andre Stewart , précédemment responsable régional des ventes chez <i>NetScreen</i>
VP Europe du Sud & MEA	Patrice Perche , ex fondateur et Président de <i>Risc Technology</i>
Directeur France	Yann Pradelle , précédemment directeur des ventes France de <i>Finjan Software</i>
Equipe 'Threat Response'	Dirigée par Guillaume Lovet , expert reconnu dans le monde de l'antivirus. Membre de l'AVIEN (Anti-virus Information Exchange Network).

Contacts relations Presse

Fortinet Barbara Maigret – Responsable Relations Presse et Analystes EMEA Tel : 04 89 87 05 52 Email : bmaigret@fortinet.com Site internet : www.fortinet.com	Point Virgule Relations Presse Elodie Repellin – Sandra Laberrenne 9, avenue de Clichy – 75017 Paris tel : 01 73 79 50 64 – 01 73 79 50 68 Email : erepellin@pointvirgule.com slaberrenne@pointvirgule.com Site internet : www.pointvirgule.fr
--	---