EXPLOITATION & ADMINISTRATION

VERS & VIRUS

Classification, lutte anti-virale et perspectives

Compléments sur le web

François Paget

DUNOD

VERS & VIRUS

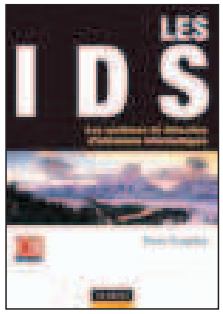
Classification, lutte anti-virale et perspectives

Consultez nos catalogues sur le Web

www.dunod.com

Sécurité des Architectures Web
Plouin, Soyer, Trioullier
496 pages
Dunod, 2004

Anti Spam : Kit de survie
Kevin Gallot
208 pages
Dunod, 2004



Les IDS
Les systèmes de détection d'intrusions informatiques
Thierry Evangelista
272 pages
Dunod, 2004

Sous la direction de
Philippe Rosé

VERS & VIRUS

Classification, lutte anti-virale et perspectives

François Paget
Chercheur anti-virus chez McAfee
Membre fondateur de l'AVERT

DUNOD

Illustration de couverture : Jeremy Woodhouse/Iguazu Falls, Brazil
Source : digitalvision®

ISBN 2 10 008311 2

Table des matières

Avant propos

L'idée d'écrire ce livre m'est venue après avoir écouté les interrogations et les commentaires de nombreux curieux. Parfois disponibles au sein d'actes de conférences quasi privés ou à l'intérieur de revues à la diffusion limitée, il m'est très vite apparu que beaucoup d'informations étaient introuvables. Cette constatation m'a encouragé à poursuivre ma démarche.

Même si mon but initial fut d'intéresser le plus grand nombre, ce livre cible un public d'informaticiens et de spécialistes. Je souhaite leur montrer une autre vision du phénomène virus : celle du *chasseur* et non pas celle du créateur. Vous n'apprendrez pas à écrire des virus mais, au fil des chapitres, vous comprendrez mieux comment on les combat.

Pour débuter notre voyage, nous positionnerons les infections informatiques dans la pyramide sécuritaire. Nous en déroulerons ses diverses facettes pour comprendre *qui est qui* et *qui fait quoi* dans cette nébuleuse malveillante.

Afin de comprendre les enjeux actuels, il est indispensable de connaître l'histoire du phénomène virus. Il s'agit d'une histoire passionnante avec une étonnante galerie de personnages. Elle est pleine de rebondissements et se rapproche parfois du triller et de la science-fiction. Par cette découverte nous entrerons dans le cœur du sujet.

Sachant ou se situe notre ennemi et quelle est son histoire, nous le décrirons dans ses multiples formes. Les divers types de virus et de vers seront déclinés selon leurs cibles et leurs attributs. Avec les virus programmes, nous rentrerons dans le cœur du métier. Ce chapitre, ainsi que celui dédié aux vers, risque d'effrayer certains lecteurs. Il me fallait trouver une méthode pour vous amener *à voir avec l'œil du chercheur*. J'ai donc manié l'hexadécimal et la visualisation des fichiers qu'il nous propose. En vous faisant appréhender la structure interne des fichiers modernes j'ai voulu donner une forte plus-value à ce livre.

Nous aborderons ensuite la protection anti-virale dans ses aspects théoriques, pratiques autant que méthodologiques. Ayant expliqué les méthodes, des pistes seront ouvertes pour aider le professionnel dans sa quête d'un bon anti-virus.

Les produits du marché sont souvent performants, ils n'excluent pas la mise en pratique de quelques conseils de configuration qui se doivent de les compléter.

Pour conclure, partant des faits marquants depuis l'an 2000, ce livre démontrera que les auteurs de virus d'aujourd'hui ne cherchent plus, ni à détruire, ni à détériorer des informations. Il mettra à jour leurs buts actuels qui, plus discrets, sont souvent bien plus préjudiciables.

Voilà donc l'itinéraire de ce livre. Pour prolonger le parcours, de nombreux liens bibliographiques vous seront offerts tout au long de votre lecture. Si le jargon technique vous laissait un temps désorienté, un glossaire que j'ai souhaité important et un index devraient vous aider à retrouver votre chemin.