



## **La décennie du cybercrime**

Cela ne fait aucun doute, le cybercrime est l'un des secteurs les plus performants et les plus lucratifs de notre époque, enregistrant une croissance à deux chiffres chaque année. Au cours des dix dernières années, l'explosion du nombre d'internautes s'est accompagnée de nouvelles formes d'attaques, de plus en plus sophistiquées. Celles-ci permettent aux cybercriminels des temps modernes de créer des logiciels malveillants leur rapportant des centaines de millions de dollars avec un risque minimum, voire nul, de se faire prendre. Pendant ce temps là, les consommateurs sont confrontés à des menaces, s'accroissant d'années en années, visant leur argent et à voler leurs informations personnelles. Alors, comment en sommes-nous arrivés là et jusqu'où ira la cybercriminalité ? Pour s'en faire une idée, revenons sur cette dernière décennie de cybercrime.

## **Les tendances 2000-2010 du cybercrime**

Au début de la décennie, les cybercriminels s'enorgueillissaient de leurs compétences en lançant des attaques qui avaient pour but de paralyser les ordinateurs des utilisateurs (généralement via des spams : e-mails contenant des pièces jointes dangereuses) ou d'arrêter temporairement des sites Web très fréquentés en les submergeant de trafic. Ils s'en sortaient bien jusqu'alors mais ces attaques ne visaient pas à faire de l'argent ; ce phénomène est apparu plus tard...

Au milieu de la décennie, les cybercriminels avaient développé différents stratagèmes profitables, dont la distribution de logiciels malveillants ou financés par la publicité, dans l'espoir d'inciter les utilisateurs à acheter le produit ou service promu. Ils parvenaient également à envoyer de grandes quantités de spams, infectant des milliers d'ordinateurs (par le biais de pièces jointes malveillantes), qu'ils pouvaient alors contrôler à distance à l'insu de leurs utilisateurs. On appelle cela des réseaux de robots (botnets), ceux-ci sont encore très actifs de nos jours. Parallèlement, la violation de données d'entreprise était pour eux un autre moyen de se faire de l'argent, par le biais de la revente de précieuses informations sur les clients.

Au cours de la seconde moitié de la décennie, les attaques se firent plus ciblées et les cybercriminels mieux organisés, allant jusqu'à former des gangs. À cette époque, les cybercriminels se servaient de l'« ingénierie sociale » pour inciter les internautes à cliquer sur des liens ou des téléchargements dangereux en évoquant des sujets et des questions qui suscitaient leur intérêt.

À la fin de la décennie, les cybercriminels s'attaquaient aussi aux utilisateurs là où ils étaient les plus vulnérables, à savoir, sur les réseaux sociaux. Les demandes émanant de faux amis, les liens dangereux et les messages d'hameçonnage qui semblaient provenir d'amis étaient autant d'outils grâce auxquels les cybercriminels accédaient aux comptes et aux ordinateurs des utilisateurs.

Par exemple, lors d'une récente arnaque par ingénierie sociale, les cybercriminels ont profité de la curiosité des utilisateurs de Facebook pour savoir qui consulte leurs profils et pour les amener à télécharger une fausse application qui était supposée leur montrer qui consultait leur page. Au lieu de l'application souhaitée, les victimes ont téléchargé un programme malveillant qui accédait à leur centre de messages Facebook pour envoyer des spams, y compris des messages qui faisaient la promotion de l'arnaque dont ils avaient été victimes.

## **Aperçu : les plus grands exploits et arnaques de la décennie**

Arnaques par rencontres en ligne -Ces arnaques courantes jouent sur les sentiments des victimes pour arriver à leur fin. L'arnaque par rencontres en ligne type consiste en un profil avec photo sur un site de rencontres en ligne dans l'espoir d'attirer les autres membres du site. L'escroc tente par la sorte, de créer des relations personnelles afin de demander de l'argent, de la marchandise ou d'autres faveurs.

Le ver « I Love You » -L'un des tous premiers exploits de la décennie (2000) fut le ver « I Love You », du nom de l'objet de l'e-mail qui le transportait. Des millions d'utilisateurs ont ouvert ce spam et ont téléchargé le fichier joint à cette « lettre d'amour » porteuse du fameux virus. Des sociétés et agences gouvernementales ont été contraintes de stopper leurs ordinateurs et ont dû déboursier 15 milliards de dollars pour se débarrasser de l'infection.

Scareware -Les cybercriminels jouent sur la peur des utilisateurs et sur le fait que leur ordinateur et leurs informations soient menacés. Les scarewares affichent des fenêtres instantanées trompeuses qui invitent leurs victimes à acheter un faux logiciel antivirus pour résoudre le problème. Cette arnaque a tellement bien marché que certains distributeurs de scarewares ont gagné des centaines de millions de dollars par ce biais.

Arnaque du Nigeria -Cette arnaque, également appelée « fraude aux frais avancés », consiste généralement en un spam provenant d'un étranger qui a besoin d'aide pour transférer des millions de dollars en dehors de son pays d'origine et qui offre au destinataire, un pourcentage de sa fortune pour l'aider. Résultat, de nombreux destinataires sont tombés dans le piège et certains ont même perdu des milliers de dollars, étant donné que les escrocs demandent une avance pour faciliter la transaction.

### **Ce que l'avenir nous réserve**

McAfee Labs s'attend à une poursuite des arnaques et des pièges sur les réseaux sociaux, notamment les demandes de faux amis, les tentatives d'hameçonnage et les liens URL dangereux sur Twitter.

Quant aux services basés sur la géolocalisation des utilisateurs tels que Foursquare et Google Places, ils présentent de nouveaux problèmes. En effet, la multiplication du nombre d'utilisateurs qui affichent publiquement leur localisation dans le monde réel, permet aux escrocs d'obtenir toutes les informations nécessaires permettant d'établir les habitudes des utilisateurs, de déterminer où ils se trouvent, à n'importe quel moment, ainsi que les moments pendant lesquels ils s'absentent de leur domicile.

La prolifération des appareils et applications mobiles est une opportunité en or pour les cybercriminels. En s'attaquant à ces équipements, les criminels peuvent ainsi voler beaucoup d'informations personnelles et bancaires à leurs utilisateurs.

Si la plupart des attaques perpétrées resteront les mêmes (hameçonnage, sites Web et téléchargements dangereux), les méthodes des cybercriminels se feront plus ciblées et plus astucieuses.