



Rapport de sécurité des TI
Publication de l'organisme-conseil

R2-002

**Logiciels malveillants : les tendances
qui se dessinent**
Rapport 2006

Sous-direction de la sécurité technique
Opérations techniques
Gendarmerie royale du Canada
Publié : août 2006

Dégagement de responsabilité

La présente publication a été préparée par la GRC à l'intention du gouvernement fédéral. Elle est officieuse et d'envergure limitée. Il ne s'agit pas d'une évaluation ni d'une approbation de technologie par la GRC. Elle représente l'opinion de la GRC formulée en fonction de l'information disponible au moment de sa rédaction. La responsabilité de toute utilisation du présent document ou de toute décision prise fondée sur ce dernier par un tiers lui revient. La GRC se dégage de toute responsabilité à l'égard des dommages que pourrait subir un tiers découlant des décisions ou des actions fondées sur la présente publication.

©Tous droits réservés 2006 Gouvernement du Canada, Gendarmerie royale du Canada (GRC)
1200, promenade Vanier, Ottawa (Ontario) Canada K1A 0R2

La présente publication peut être reproduite intégralement sans frais à des fins éducatives et personnelles seulement. Toutefois, l'autorisation écrite de la GRC est requise pour utiliser ce document sous forme révisée ou d'extraits, ou à des fins commerciales.

TABLE DES MATIÈRES

SOMMAIRE	1
1 Introduction	2
2 Objectif	2
3 Caractéristiques des maliciels.....	3
3.1 Nouvel objectif des maliciels.....	3
3.2 Déclin de l'épidémie.....	3
3.3 Temps de création des maliciels.....	3
3.4 Types de maliciels et vecteurs de propagation.....	4
3.5 Modularité des maliciels.....	4
4 Tendances qui se dessinent	5
4.1 Téléphones cellulaires et appareils mobiles	5
4.2 Médias portatifs.....	5
4.3 Technologies Rootkit	6
4.4 Refus de service distribué sur demande.....	7
4.5 Extorsion par crypto virus et « ransomware ».....	7
4.6 Nouvelles technologies et tactiques de ciblage	7
4.7 Maliciels libres	8
4.8 Nouvelles méthodes d'hébergement poste à poste.....	8
4.9 Maliciels à vendre	9
4.10 Maliciels dans les applications Web	9
4.11 Identification par radio-fréquence comme vecteur de propagation	10
5 Conclusion.....	11
6 Glossaire.....	11

SOMMAIRE

Les logiciels malveillants (maliciels) représentent une grande menace pour les systèmes d'information du monde entier. Se tenir au courant dans le domaine des maliciels peut s'avérer très difficile, car ceux-ci évoluent à un rythme effréné. Le présent document vise à donner un aperçu des tendances des logiciels malveillants qui, selon les chercheurs et les experts, toucheront l'infrastructure mondiale de l'information au cours de l'année à venir. On y décrit également quelques-unes des caractéristiques actuelles des logiciels malveillants qui sont en circulation dans le monde. Aujourd'hui, les maliciels changent plus rapidement, ils ont une conception modulaire et ils se propagent au moyen de méthodes nouvelles et inédites. D'autre part, l'objectif primaire des maliciels a changé au cours des dernières années. De plus en plus, la tendance est à la création de logiciels malveillants à des fins lucratives au profit de leurs auteurs.

On s'attend à ce que la création de maliciels évolue sans cesse et à ce qu'apparaissent de nouvelles façons d'exploiter les systèmes informatiques, de les infecter et d'en faire des victimes. Un grand nombre de tendances décrites dans le présent document traitent des nouvelles façons de se servir des maliciels pour en tirer profit, qu'il s'agisse de la vente de logiciels malveillants à des délinquants sur le marché noir ou de la location de l'utilisation des systèmes qui en sont victimes. Quelques auteurs de maliciels ont recours à de nouvelles technologies comme les « rootkits » pour cacher leur virus, alors que d'autres facilitent la création de nouveaux maliciels en diffusant leur code source de logiciel d'exploitation libre du domaine public (GNU) comme un logiciel libre. Les vers et les virus se répandent de plus en plus sur d'autres plateformes, telles que, sans toutefois s'y limiter, les téléphones cellulaires, les assistants numériques, les clés USB et même les puces d'identification par radio-fréquence.

Il est de plus en plus difficile de retracer les maliciels et de les prévoir, car leur développement est de plus en plus organisé et bien financé par les organisations criminelles. Il faudra poursuivre la recherche et continuer à agir avec prudence afin de mieux comprendre ces menaces, et le présent document servira de bon point de départ. Entre-temps, les logiciels malveillants continuent de s'attaquer aux systèmes qui résistent le moins. Il faut installer des programmes antivirus et des pare-feu et les tenir à jour; les utilisateurs doivent faire preuve d'une prudence constante lorsqu'ils sont en ligne. Enfin, les mises en garde émanant des fournisseurs et des centres gouvernementaux, tels que le Centre canadien de réponse aux incidents cybernétiques (CCRIC), devraient être prises en compte.

1 Introduction

Les logiciels malveillants sont généralement reconnus comme la plus grande menace pour la sécurité des systèmes informatiques du monde entier depuis plusieurs années déjà¹.

Étant donné que les systèmes d'ordinateurs du gouvernement sont branchés directement ou indirectement à Internet public, ils peuvent être très vulnérables à un éventail de menaces connues sous le nom de logiciels malveillants, autrement appelés « maliciels ». Les conséquences d'un incident de sécurité dans le domaine de la technologie de l'information (TI) causé par un maliciel peuvent varier selon le degré de l'impact « peu important » ou « important ». Il est du plus haut intérêt de tous les ministères fédéraux de faire preuve de la « diligence raisonnable » pour éviter que les maliciels touchent la confidentialité, l'intégrité et la disponibilité des services qu'ils fournissent et les données qu'ils protègent.

Jusqu'à une époque récente, la grande majorité des attaques venant d'Internet auxquelles les systèmes ont fait face étaient très automatisées et n'étaient pas ciblées. Bien que les systèmes du gouvernement aient pu faire l'objet d'attaques ciblées, ils étaient encore plus exposés à des vérifications systématiques de la part d'autres systèmes infectés. Cependant, le paysage des logiciels malveillants est en voie de changement. Les attaques sont de plus en plus spécialisées, alliant l'ingénierie sociale à d'autres méthodes qui permettent de passer outre les systèmes de défense. Les attaques sont de plus en plus ciblées, et les systèmes de stockage de données confidentielles sont très prisés.

L'une des raisons primordiales pour lesquelles les logiciels malveillants représentent encore une si grande menace, c'est la vitesse avec laquelle ils se vendent et sont modifiés. Qui plus est, nous assistons aujourd'hui à des innovations, car les logiciels malveillants ne sont plus des moyens de perturber les systèmes informatiques et d'interrompre les communications, mais des « outils de la criminalité » pour les inondeurs, les pirates informatiques et les criminels organisés. Ces « outils » renforcent la capacité de ces personnes de générer des millions de dollars en profits illicites.

2 Objectif

Le présent rapport vise à donner un aperçu de l'évolution et des nombreuses tendances des logiciels malveillants que les experts observent actuellement, et des tendances auxquelles ils s'attendent dans l'avenir prévisible². Ce n'est pas un document qui trace l'avenir des logiciels malveillants, car il serait impossible de le faire. Les créateurs de maliciels se déplacent très rapidement. Ils sont capables de s'adapter et, très souvent, ils exploitent les vulnérabilités avant que le reste de l'industrie de la sécurité ne soit pleinement au courant de leur existence³. Il leur est essentiel de faire preuve de souplesse et de réagir rapidement s'ils souhaitent continuer à faire des profits et à devancer les fournisseurs d'antivirus qui mettent au point constamment de nouvelles méthodes de détection et de suppression de programmes nuisibles⁴. Par conséquent, il se peut que certaines tendances mentionnées dans le présent document n'aient jamais lieu alors que d'autres, qui n'ont pas été mentionnées, feront sans aucun doute leur apparition.

Le présent document donnera au lecteur une meilleure opinion des enjeux en présence, et peut-être une meilleure idée de la façon de s'y retrouver dans les logiciels malveillants de demain.

3 Caractéristiques des maliciels actuels

3.1 Nouvel objectif des maliciels

Les logiciels malveillants ont connu une transformation clé au cours des dernières années. Le temps où les virus et les vers étaient nantis de charges dont le seul but était de détruire des données, de faire se planter des systèmes informatiques ou de couper les communications, est en grande partie révolu. Bien que les maliciels destructifs continuent à être très courants, il y a eu une augmentation visible du nombre de logiciels malveillants qui ne sont pas porteurs de charges destructives. Il est clair qu'il y a un intérêt accru à maintenir le système de la victime en ligne et opérationnel⁵. La tendance est de plus en plus à écrire des logiciels malveillants à des fins lucratives⁶.

Aujourd'hui, les logiciels malveillants font profiter leurs auteurs de plusieurs façons différentes. L'une des méthodes les plus courantes est de voler des renseignements délicats pour les vendre ensuite à des organisations criminelles sur le marché noir. Des renseignements comme des numéros de carte de crédit et d'assurance sociale, des noms d'utilisateur et des mots de passe, et d'autres fichiers de nature délicate sauvegardés sur des disques durs, sont volés et monnayés facilement⁷. Le secteur financier est une des cibles les plus frappées. Il n'est pas surprenant que les programmes du type cheval de Troie qui ciblent particulièrement les noms d'utilisateur et les mots de passe dans les sites Web des banques aient connu une croissance soutenue pendant les deux ou trois dernières années⁸. Une autre méthode courante est d'utiliser des logiciels robots pour forcer le système de la victime à joindre un réseau de robots. On dit que les réseaux de zombies qui sont surveillés par les fournisseurs d'antivirus et les organismes d'application de la loi regroupent souvent plus de 30 000 à 40 000 systèmes. (On dit qu'un des plus grands réseaux de zombies ayant jamais été découverts contrôlait 100 000 systèmes zombies)⁹. Ces réseaux de systèmes peuvent être utilisés pour lancer des attaques de refus de service distribué, abriter du matériel illégal et envoyer des pourriels.

Au cours des dernières années, les logiciels malveillants ont montré qu'ils étaient une bonne méthode de faire de l'argent pour les entrepreneurs criminels. L'aspect profitable des maliciels est là pour rester.

3.2 Déclin de l'épidémie

Les épidémies de vers ont été le fléau d'Internet pendant des années. Cela a commencé avec le vers Morris, en 1988, et a continué plus tard avec Melissa, le virus I LOVE YOU et bien d'autres. Cependant, au cours des deux dernières années, il y a eu une réduction marquée du nombre d'épidémies. Selon toute probabilité, cela peut s'expliquer par le fait que la sécurité des systèmes d'exploitation s'est accrue et que des progrès ont été réalisés dans la technologie de l'antivirus¹⁰. En même temps, les maliciels ont eux aussi changé, en raison de l'évolution de la dynamique sociale. De nombreux logiciels malveillants qui apparaissent dans Internet aujourd'hui sont dirigés vers quelques cibles seulement. Cela veut dire qu'un pirate informatique peut façonner son maliciel de manière à utiliser des astuces d'ingénierie sociale plus sophistiquées afin de duper les utilisateurs. Cela est devenu nécessaire, car les utilisateurs apprennent de plus en plus à laisser de côté les courriels et les messages non sollicités¹¹. Cibler moins de victimes veut également dire que les fournisseurs d'antivirus ne verront pas un maliciel aussi tôt qu'ils ne l'auraient vu si le programme avait été diffusé partout dans Internet¹². Cela élargit les possibilités des auteurs de maliciels avant même que les fournisseurs d'antivirus ne mettent à jour leur signature de détection.

3.3 Temps de création des maliciels

Le monde d'Internet a pris de la vitesse au cours des dernières années et, semble-t-il, les logiciels malveillants aussi. Lorsqu'une vulnérabilité est annoncée publiquement, les créateurs de maliciels et les fournisseurs de logiciels se font la course. Les auteurs de maliciels sont de plus en plus perspicaces à produire des programmes malveillants avant que les entreprises ne produisent des sous-programmes de correction.

Quand le ver Nimda a été découvert en septembre 2001, on connaissait la vulnérabilité qu'il exploitait depuis 366 jours. Microsoft avait produit un sous-programme de correction en octobre 2000. Les administrateurs avaient près d'un an pour colmater la brèche de sécurité. Quatre ans plus tard, le ver Zotob a été découvert, circulant librement. Cette nouvelle vulnérabilité n'était connue du public que depuis quatre jours¹³.

Le délai de création de programmes malveillants qui exploitent des vulnérabilités rendues publiques se raccourcit d'année en année, ce qui fait que les possibilités d'exploiter les systèmes vulnérables ont augmenté. Bien que le délai d'exploitation se soit récemment allongé (6,4 jours en moyenne), il est encore très court comparé à la moyenne de 49 jours dont les fournisseurs ont besoin pour produire des sous-programmes de correction des vulnérabilités rendues publiques¹⁴.

3.4 Types de maliciels et vecteurs de propagation

Plusieurs autres changements ont eu lieu dans le monde des logiciels malveillants. Au cours des dernières années, la catégorie « classique » des logiciels malveillants, soit la catégorie des « virus », est en véritable déclin.¹⁵ Cela est dû au fait que, à ce jour, de nombreux virus se sont typiquement répandus lentement ou ont porté des charges destructives. Les vers, les chevaux de Troie et les robots d'exploitation d'aujourd'hui se déplacent beaucoup plus rapidement et offrent la fonctionnalité d'en tirer des profits.

Les vecteurs de propagation ont eux aussi changé récemment. Le nombre de vers qui se propagent dans les réseaux de partage de fichier poste à poste a chuté considérablement au cours des deux ou trois dernières années. On a attribué la raison principale de cette chute aux efforts déployés par certaines organisations, comme celles qui sont responsables de la protection des droits d'auteur dans les industries du film et de la musique. Le vide a été comblé par les vers et les logiciels malveillants qui se propagent dans les réseaux de messagerie instantanée (MI). En 2004, la société Kaspersky Labs a constaté qu'il y avait en moyenne un nouveau ver de MI par mois¹⁶. En 2005, la moyenne aurait sauté à vingt-huit par mois. On prévoit que cette activité va augmenter parce qu'on s'attend à ce que le trafic de la messagerie instantanée dépasse celui du courrier électronique au cours de l'année 2006. Quelques vers de MI peuvent envoyer des messages à toutes les personnes dont le nom figure sur la liste de contacts d'un utilisateur. D'autres vers sont capables de « clavarder » avec des victimes, les incitent à cliquer sur un lien malveillant. Le fait que la plupart des personnes font naturellement confiance aux noms qui se trouvent dans leur liste de contacts ne fait que rendre les attaques par MI plus efficaces¹⁷.

3.5 Modularité des maliciels

Les maliciels ne relevaient autrefois que du monde des programmeurs qualifiés. Ceux-ci étaient capables de créer un programme à partir de zéro, car ils comprenaient les langages de programmation ainsi que les notions de réseautage et de système nécessaires à la création de logiciels malveillants fonctionnels. Avec le temps, les modes d'emploi et les tutoriels sont devenus monnaie courante, et ceux qui ont besoin d'aide peuvent se les approprier¹⁸.

Aujourd'hui, il semble que nous entrons dans l'ère des maliciels modulaires et des « trousseaux » de virus. Les maliciels « modulaires » sont souvent définis de deux façons différentes. Premièrement, certains maliciels sont écrits de façon modulaire. Aujourd'hui, les composants et les charges associés aux programmes malveillants sont disponibles en modules qu'on introduit dans la mémoire ou qu'on en sort facilement. Ainsi, de nombreuses combinaisons de fonctions et de charges sont immédiatement réalisables. On l'a d'ailleurs souligné comme suit dans un journal : [Traduction] « (Si vous) désirez avoir la possibilité de propager (les maliciels) poste à poste, ajoutez-la ; (Si vous) voulez les diffuser par MI, c'est fait¹⁹. » La création de maliciels a maintenant atteint l'étape où il suffit de pointer-cliquer pour concevoir un nouveau ver. Les trousseaux de maliciels mettent même à la disposition de l'utilisateur une interface Windows et des cases à cocher pour inclure ou exclure des charges et des méthodes de

propagation différentes²⁰. Le deuxième type de maliciels modulaires a trait aux maliciels qui se servent de la « modularité » pour améliorer leur fonctionnalité une fois qu'un système est compromis. Par exemple, les maliciels peuvent être programmés de façon à rester petits (moins de 50 Ko), furtifs et très mobiles. L'objectif est simplement de s'implanter dans le système²¹. À partir de là, le ver ou le cheval de Troie communiquera avec des serveurs branchés à Internet afin de télécharger des modules de programmes et d'augmenter ainsi sa fonctionnalité. De nombreux logiciels robots ont des instructions incorporées au programme, ce qui leur permet d'entrer en communication avec des canaux de logiciels de conversation en ligne (Internet Relay Chat ou IRC) et d'attendre de recevoir des consignes. C'est une méthode très efficace d'ajouter de la fonctionnalité puisque, à partir de son centre d'opération, le « propriétaire » du réseau de zombies peut envoyer l'ordre aux logiciels robots qui écoutent de télécharger des modules précis. Les programmes ainsi téléchargés peuvent contenir des mises à jour des maliciels eux-mêmes, des enregistreurs de frappes, des serveurs mandataires, des logiciels de publicité, des logiciels espions et d'autres logiciels criminels qui permettent de faire des profits illégaux²².

4 Tendances qui se dessinent

4.1 Téléphones cellulaires et appareils mobiles

Les auteurs de maliciels sont constamment à l'affût de nouvelles cibles vulnérables à exploiter – surtout qu'à l'heure actuelle, les logiciels malveillants sont monnayables. Les maliciels qui s'attaquent aux appareils mobiles représentent une menace grandissante depuis quelques années. On croit qu'il y a au delà de cent variantes de logiciels malveillants qui sont déjà en circulation et qui exploitent les appareils mobiles, comme les téléphones cellulaires et les assistants numériques²³. Ces variantes sont responsables d'avoir endommagé des appareils mobiles, d'avoir supprimé des données et d'avoir compromis des renseignements délicats et, maintenant, il existe des variantes qui peuvent sauter d'un appareil mobile à un ordinateur de bureau utilisant Windows²⁴.

À mesure que les fournisseurs de téléphones cellulaires ajoutent des passerelles Internet et d'autres services pour améliorer la performance et la fonctionnalité²⁵, l'intérêt porté aux appareils mobiles augmente. On s'attend toutefois à une hausse considérable à mesure que les utilisateurs d'appareils mobiles auront accès aux services bancaires et aux services de paiement à partir de leurs téléphones cellulaires. Cela aura pour conséquence, sans aucun doute, de générer plus d'intérêts de la part des éléments criminels. Cette nouvelle menace est d'autant plus aggravée par le fait que les utilisateurs ne sont pas généralement conscients de la sécurité et qu'ils ont tendance à accepter les messages non sollicités qu'ils reçoivent²⁶.

4.2 Médias portatifs

Bien qu'il ne s'agisse pas explicitement d'une question de logiciels malveillants, c'est certainement une question de sécurité que les logiciels malveillants pourraient exploiter dans l'avenir. Les appareils de médias portatifs, comme les clés USB et les puces mémoires, existent depuis un certain nombre d'années. Ils ont évolué au point où ils peuvent contenir une quantité considérable de données, et où ils sont extrêmement faciles à dissimuler et à installer. La menace dans ce cas se présente sous forme d'un modèle connu sous le nom de « Pod Slurping » (espionnage via iPod)²⁷. Le but est d'utiliser un baladeur numérique de type iPod pour copier les fichiers d'un ordinateur, puis de quitter les lieux avec un appareil qui, d'après ce que la plupart des gens pensent, ne contient que de la musique. Les maliciels peuvent exploiter ces vulnérabilités de deux façons différentes.

Premièrement, ils peuvent apprendre à avoir un accès superposé au système informatique d'une organisation. En infectant le lecteur portatif de l'utilisateur chez lui²⁸, les maliciels ainsi cachés passeront par le contrôle d'accès externe de l'entreprise, et ce, à l'insu de leur utilisateur. À partir de là, le ver aura

la liberté d'attaquer l'infrastructure informatique par l'intérieur même de l'entreprise, c'est-à-dire là où il y a souvent moins de protection. On souligne ici le fait que cela sera un moyen pour les logiciels malveillants de pouvoir s'infiltrer dans un réseau que l'on estime hautement sécuritaire. En utilisant l'idée des attaques « à 180 degrés »²⁹, un concept présenté lors de la conférence Black Hat USA en 2002, le programme explorera les voies de sortie du réseau pour communiquer avec son point d'origine et commencer à voler des données délicates.

La deuxième possibilité est peut-être plus insidieuse. Le même scénario serait joué, sauf que l'utilisateur apporterait consciemment au bureau le logiciel malveillant qui se trouve sur son média portatif. Ayant personnellement créé le logiciel malveillant, ce qui est d'une facilité déconcertante aujourd'hui, l'utilisateur malveillant pourrait ensuite l'introduire dans le réseau interne. Il pourrait soit répandre l'« infection » lui-même en accédant personnellement à une multitude de systèmes, soit programmer le maliciel de façon à ce qu'il se répande sournoisement partout dans le réseau et s'assurer qu'il n'a pas dépassé les frontières du réseau local (RL) de l'entreprise. Une fois que le maliciel est installé sur une multitude de systèmes, l'employé malintentionné n'aura qu'à attendre que le programme renvoie des fichiers de nature délicate à l'appareil média portatif. Après avoir fini le vol, le ver pourra s'effacer, et l'employé pourra sortir des lieux avec un appareil sur son porte-clés, que les gens prendront pour un surligneur de poche au lieu d'un appareil de stockage qui renferme un nombre incalculable de fichiers de nature délicate.

4.3 Technologies Rootkit

Il est normal que plus un maliciel peut rester dans un système infecté sans être détecté, plus il sera efficace (ou, comme c'est le cas aujourd'hui, plus il rapportera de l'argent)³⁰. Le fait que le nombre de rootkits détectés sur des systèmes compromis est à la hausse depuis peu ne devrait surprendre personne. C'est une tendance très inquiétante, car les rootkits peuvent être très difficiles à déceler et peuvent être utilisés pour camoufler d'autres types de maliciels. Les fournisseurs d'antivirus ont déjà commencé à faire remarquer qu'à leurs avis, les rootkits constituent une véritable menace future³¹.

Plus inquiétantes, peut-être, sont les récentes découvertes des chercheurs dans le domaine. Des spécialistes et des étudiants d'université ont découvert et mis au point de nouvelles technologies de rootkits qui rendront la détection des maliciels encore plus difficile. Microsoft et des étudiants de la University of Michigan ont réussi à créer, comme validation de principe, une machine virtuelle rootkit qui peut fonctionner à l'extérieur des limites du système d'exploitation. Le rootkit crée une couche séparée, un moniteur de machine virtuelle (MMV), entre le matériel et le système d'exploitation. Au démarrage du système, le système d'entrée-sortie de base (BIOS) remet le contrôle de l'ordinateur au MMV, déjouant ainsi le processus normal de lancement. Une fois le processus de lancement terminé, toute interaction entre l'utilisateur et l'ordinateur s'effectue au moyen du MMV³².

Peu avant que cette recherche ne soit mise à jour, un conférencier à la conférence Black Hat a présenté le concept du camouflage des rootkits dans le BIOS d'un ordinateur. Bien qu'il n'ait existé que relativement peu de logiciels malveillants qui tentent de modifier le BIOS, la menace est considérée plausible, puisque l'accès au langage de programmation (ACPI), aux compilateurs et aux instructions est très facile. D'autres chercheurs qui assistaient à la conférence n'ont pas été d'accord quant aux chances d'un maliciel automatisé de pouvoir répandre un tel rootkit, en raison des mécanismes de sécurité du matériel informatique. Néanmoins, la menace serait certainement plausible si une personne de l'intérieur installait le rootkit elle-même. Si le rootkit était installé sur un ordinateur portatif, par exemple, il pourrait être utilisé comme une porte dissimulée de l'organisation, bien après que l'utilisateur a arrêté d'utiliser le système. Un tel rootkit serait capable de subsister même si les disques durs sont reformatés ou remplacés; ce serait donc un maliciel très résistant³³.

4.4 Refus de service distribué sur demande

Pendant des années, les délinquants ont eu recours à l'extorsion pour intimider les gens et faire de l'argent. Depuis deux ou trois ans, les délinquants informatiques ont perfectionné leur capacité d'extorquer de grosses sommes à des entreprises en ligne, en échange de la « protection » des sites Web de ces entreprises. Celles-ci reçoivent normalement un courriel selon lequel on les informe qu'elles doivent verser une somme pour se protéger ou faire face à une attaque de refus de service distribué qui mettra leurs sites Web hors ligne. Avec la taille des logiciels robots d'aujourd'hui, un grand nombre de ces menaces semblent très plausibles. Bien que les attaques de refus de service aient existé pendant des années, ce n'est que depuis un an ou deux que ces activités d'extorsion sont montées en flèche³⁴.

Les groupes de crime organisé ont commencé à contrôler ou à louer des logiciels robots afin de s'en servir pour leurs attaques. Cette entreprise est nettement profitable, quoique illégale. LA National Hi-Tech Crime Unit (NHTCU) au Royaume-Uni a déclaré avoir arrêté un groupe de crime organisé russe qui avait extorqué 1,3 million de livres sterling en 90 jours³⁵.

Il est probable, croit-on, que la hausse du nombre d'attaques peut être attribuée au fait que de nombreuses organisations pensent qu'il est plus facile de verser une somme pour leur protection que d'investir davantage dans la défense de leurs bandes passantes ou de perdre complètement l'accès à leur site Web. Certains experts croient que, à mesure que les extorqueurs rentabilisent leurs efforts et que leurs logiciels robots progressent en complexité et en puissance, cette tendance continuera progressivement à se généraliser³⁶.

4.5 Extorsion par crypto virus et « ransomware »

Pendant longtemps, le chiffrement a été perçu comme une technologie défensive. On garde les fichiers loin des regards indiscrets et seules les personnes qui ont l'autorisation de voir les renseignements en détiennent la clé. Toutefois, on a éventuellement reconnu que la cryptographie pouvait également être utilisée comme technologie offensive³⁷. Si la mauvaise personne détenait la seule clé aux données chiffrées, il serait alors possible qu'elle fasse des demandes avant de retourner les données. Le cheval de Troie AIDS, qui a été découvert en 1989, était le premier logiciel malveillant à infecter un système et à chiffrer le disque dur par la suite afin de tenter d'exiger une rançon pour les données³⁸. Les programmes de crypto virus n'ont pas représenté une grande menace dans les années quatre-vingts et quatre-vingt-dix. Cependant, au cours de l'an dernier, plusieurs programmes du type « ransomware » ont été découverts par les fournisseurs d'antivirus. Il semble que ces programmes sont de plus en plus populaires.

Ces exemples récents de « ransomware » ont montré que les algorithmes cryptographiques ne sont pas encore au point et que, dans certains cas, la clé de déchiffrement reste cachée dans le système de la victime³⁹. Bien qu'il n'y ait eu que relativement très peu d'exemples de ce genre de menaces à ce jour, il est clair que les programmeurs malveillants font présentement des expériences et qu'ils commencent à apprendre. À mesure que les techniques de dissémination et de chiffrement s'améliorent et si les tentatives d'extorsion commencent à aboutir, cela pourrait vite devenir un phénomène plus courant.

4.6 Nouvelles technologies et tactiques de ciblage

Comme la criminalité s'est tournée vers le monde en ligne, les fournisseurs et les commerçants ont commencé à se défendre. Les entreprises emploient de plus en plus la technologie de géolocalisation sur protocole Internet (IP) afin de déterminer la situation géographique d'un acheteur potentiel, et ce, en vue de réduire les achats frauduleux. Plusieurs entreprises ont compilé d'énormes bases de données qui leur donnent la possibilité de retracer une adresse IP tout au moins à son pays d'origine⁴⁰. Malheureusement, les commerces en ligne ne sont pas les seuls qui peuvent se servir de cette technologie de géolocalisation sur IP. Avec l'ingénierie sociale qui s'avère être un grand vecteur d'attaques de maliciels, l'information devient un atout très important. Plus les pirates informatiques acquièrent des renseignements sur une

cible, plus leur attaque est efficace. Aujourd'hui, les services de géolocalisation sur IP sont incroyablement précis. Ils peuvent révéler le nom du pays, de la région et de la ville, le code postal, la latitude et la longitude, le nom du fournisseur d'accès Internet (FAI) et le nom de l'entreprise associée à une adresse IP en particulier. Tous ces renseignements sont offerts à des prix relativement bas, et un nombre limité de recherches peuvent même être faites gratuitement⁴¹.

D'autres technologies commenceront également à avoir un effet grandissant sur la puissance des vers, des virus et des logiciels robots qui parviennent à nos ordinateurs. Pendant des années, un des signes les plus révélateurs de la présence d'un ver dans notre courrier électronique était le nombre de fautes d'orthographe et de grammaire dans le corps de message. Maintenant, les créateurs de maliciels utilisent les correcteurs grammaticaux et de langue⁴² et créent des vers qui peuvent parvenir au système en plusieurs langues et l'attaquer dans la langue qu'ils ont détectée dans le système de la victime.

Une autre tactique qui a été utilisée pendant de nombreuses années a été celle de profiter des grands événements et des actualités mondaines pour tromper la vigilance des utilisateurs. Jusqu'à maintenant, ce phénomène n'a pas eu de cible en particulier, et le courrier électronique infecté était envoyé partout dans le monde⁴³. Les nouvelles technologies qui repèrent les adresses IP rendent ces attaques beaucoup plus efficaces. En se servant de la quantité de mouvements d'un événement dans un lieu donné, les créateurs de logiciels malveillants pourront créer un maliciel et le répandre en ciblant un segment très précis de la population mondiale. Cela ferait paraître les courriels encore plus légitimes. On a déjà trouvé des courriels en vente en ligne qui distinguent non seulement les pays et les villes, mais aussi les industries⁴⁴. Cela pourrait être le début de la croissance du commerce clandestin et de la vente de renseignements de ciblage.

4.7 Maliciels libres

Les logiciels malveillants en sont aujourd'hui au stade où presque tout le monde y a accès. Les maliciels sont maintenant dévoilés en tant que GNU. Non seulement n'importe qui a le droit de modifier et de lancer ces logiciels dans Internet, mais on est en fait encouragé à le faire. Cette situation pourrait expliquer la chute soudaine du nombre de familles de logiciels malveillants en circulation dans la seconde moitié de l'année 2005, alors que le nombre de variantes de ces familles a continué à grimper tout au long de 2005⁴⁵. Tous genres de maliciels ont été ouverts au moyen de GNU, y compris les vers, les virus, les chevaux de Troie, les Remote Acces Trojans (Trojans d'accès à distance)⁴⁶ et les rootkits⁴⁷.

C'est une initiative intéressante de la part des concepteurs de maliciels expérimentés, fait remarquer Dancho Danchev, directeur général d'Altavista.com. Dans cette nouvelle situation, des centaines d'auteurs inexpérimentés courent une plus grande chance d'être attrapés que les vétérans. Toutes les variantes qui apparaissent sur le marché attirent tellement d'attention que les auteurs plus expérimentés peuvent rester dans l'ombre. En théorie, cela permettrait même aux véritables auteurs de détourner les meilleures mutations de leurs programmes originaux⁴⁸.

4.8 Nouvelles méthodes d'hébergement poste à poste

Le nombre de clients poste à poste et le nombre de réseaux qui hébergent des fichiers de contenu multimédia et d'autres données ont visiblement baissé. Les organisations responsables de lutter contre les violations du droit d'auteur travaillent sans relâche en vue de fermer le plus grand nombre possible de réseaux et d'arrêter les principaux intervenants dans le monde du poste-à-poste. Il n'est donc pas surprenant d'apprendre que les vers poste à poste ne sont plus aussi populaires⁴⁹.

Sans être découragées par ces coups de filet, les têtes de réseau de zombies semblent avoir commencé à trouver un moyen de contourner le problème. La solution part du nombre assez important de réseaux de zombies qui existent déjà dans Internet. Ce grand nombre d'ordinateurs offrent d'immenses espaces disques et de bandes passantes à profusion – l'endroit idéal pour voiler les nouveaux réseaux poste à

poste. Imaginez un immense entrepôt dynamique où sont stockées toutes sortes de matériel illégal⁵⁰. Ce serait un système dans lequel des hôtes seraient constamment ajoutés, et la perte d'un hôte ou deux n'aurait pas d'effet sur l'ensemble du réseau. La technologie BitTorrent permettrait le transfert de très grands fichiers, et le chiffrement et l'authentification des mots de passe pourraient être utilisés pour garder le réseau encore plus loin des regards indiscrets. Un tel réseau a déjà été découvert. On s'est aperçu qu'un réseau de zombies placé sous surveillance téléchargeait des fichiers de films à partir de systèmes attaqués. Les propriétaires du réseau de zombies utilisaient une version personnalisée du logiciel BitTorrent pour télécharger des fichiers assez considérables sans éveiller les soupçons de leur victime. Un autre aspect inquiétant de cette situation est que, en installant le logiciel BitTorrent, les pirates informatiques sont maintenant en mesure de semer, dans les ordinateurs attaqués, de plus gros paquets de maliciels⁵¹.

4.9 Maliciels à vendre

En un sens, la sécurité informatique est bien une affaire de rapidité ; la rapidité avec laquelle un pirate informatique crée un logiciel en vue d'exploiter une vulnérabilité, la rapidité avec laquelle une entreprise émet un sous-programme de correction ou la rapidité avec laquelle une organisation peut faire parvenir des renseignements au grand public. Une façon dont certaines entreprises ont abordé cette question d'exploits du jour zéro, c'est de commencer à offrir une récompense monétaire en échange de renseignements sur des vulnérabilités non publiées de programmes logiciels. Cela leur permet de donner les renseignements à leurs propres clients avant de les donner au reste du monde. Le délai moyen pour publier un exploit s'est allongé légèrement au cours des derniers mois. Cela pourrait s'expliquer par le fait que les pirates informatiques expérimentés et les chercheurs font maintenant connaître leurs exploits à des entreprises privées contre rémunération⁵². Cela soulève toutefois la question suivante : si les chercheurs sont prêts à vendre leurs connaissances à des entreprises privées, qu'est-ce qui les empêcherait de les vendre sur le marché noir? Les entreprises de crime organisé seront toujours à même d'offrir plus d'argent et d'autres primes d'encouragement en échange de ces renseignements si précieux. Il est clair que le marché se fait déjà exploiter. La vulnérabilité du métafichier de Windows (MS06-001), qui a été découverte à la fin de décembre 2005, avait déjà été utilisée pendant des semaines. Des pirates informatiques en Russie ont découvert cet exploit au début du mois de décembre et l'ont proposé ensuite à des groupes de crime organisé pour 4 000 \$. L'information sur cette vulnérabilité n'avait jamais été passée aux entreprises de sécurité du secteur privé. Plusieurs semaines se sont écoulées avant que les fournisseurs d'antivirus ne prennent connaissance de cette vulnérabilité ainsi que des logiciels d'exploitation connexes. Des sites Web comme Shadowcrew.com et Carderplanet.com étaient les premiers à exploiter ce marché illégal et offraient dans leurs sites, sur demande, des programmes de piratage, des maliciels et des outils de cartes de crédit frauduleuses, jusqu'à ce qu'ils soient arrêtés par le service secret des États-Unis⁵³.

Le marché clandestin est en plein essor pour ces genres d'arrangements entre acheteurs et vendeurs⁵⁴, ce qui accélérera vraisemblablement la création de logiciels d'exploitation privés que les entreprises de sécurité devront découvrir à leurs dépens.

4.10 Maliciels dans les applications Web

Dans la section Caractéristiques des maliciels actuels de la présente publication, nous avons souligné que le nombre d'épidémies de vers et de virus avait nettement chuté récemment et qu'un changement de tactiques semblait s'opérer dans le monde des maliciels en vue de mieux cibler les attaques et de mieux les situer géographiquement. Cependant, une mise en garde s'impose. Dans la collectivité de la sécurité informatique, on croit toujours qu'on n'a pas encore vu la dernière des épidémies d'envergure de vers.

Les administrateurs de réseau ont bloqué les points d'accès communs en vue de couper les voies de communication empruntées par les logiciels malveillants, et les pirates informatiques ont dû changer de

tactiques pour y remédier. Les experts s'attendent à ce que les nouvelles vulnérabilités qui seront exploitées soient celles que l'on trouve dans les applications Web⁵⁵. Ces brèches de sécurité offrent la possibilité aux logiciels malveillants d'atteindre un nombre incroyable de victimes en un temps très court, et ce genre de menaces peut être très difficile à contrer. En exploitant la vulnérabilité d'une application Web dans un site très achalandé, les pirates seraient à même d'atteindre un très grand nombre d'utilisateurs. Certains experts prévoient que cela pourrait se réaliser par voie de mystification du contenu⁵⁶ ou de vulnérabilités du type « Cross-Site Scripting »⁵⁷. Une vulnérabilité de ce type a été découverte dans un des serveurs de Yahoo. Si elle avait été exploitée, des millions d'utilisateurs auraient été redirigés vers toutes sortes de logiciels malveillants⁵⁸.

Un facteur qui aggrave le problème, c'est le fait que les applications Web ont normalement une façade dans Internet et qu'elles interagissent en même temps avec des serveurs internes dorsaux. Une entreprise en ligne ne peut simplement pas bloquer tous les points d'accès communs (p. ex. le port 80, HTTP) que les clients utilisent pour avoir accès à ses serveurs. Cette raison, en plus du fait que le trafic sur le Web peut être très compliqué, fait que la détection et la protection contre les exploits Web peuvent s'avérer très difficiles⁵⁹.

Les fournisseurs d'antivirus ont déjà classé plusieurs logiciels malveillants qui exploitent les vulnérabilités des applications Web. Le fait que les auteurs de logiciels malveillants se servent déjà de ce vecteur d'attaque ne devrait surprendre personne. La prochaine vulnérabilité grave d'une application Web suscitera sans aucun doute beaucoup d'intérêt auprès des auteurs de logiciels malveillants et générera beaucoup de logiciels malveillants.

4.11 Identification par radio-fréquence comme vecteur de propagation

On s'attend à ce que la technologie de l'identification par radio-fréquence (IRF) prenne la relève des codes à barres au cours des prochaines années. Les IRF permettent de vérifier facilement et rapidement l'inventaire des produits dans les entrepôts et de simplifier le passage à la caisse dans les magasins de détail. Cependant, des recherches récentes ont révélé que l'IRF n'est pas une technologie complètement inoffensive. Les balises des IRF communiquent avec le même genre de serveurs de base de données dorsaux que les serveurs utilisés par d'autres technologies, comme les serveurs Web. Les balises des IRF peuvent aussi être réécrites et peuvent comprendre de petites quantités de données⁶⁰. Il n'est pas surprenant que des chercheurs aient découvert que l'IRF peut être exploitée de la même manière que d'autres technologies. Des surcharges de la mémoire tampon, des attaques par injection de langage relationnel SQL (SQL) et même des logiciels malveillants capables de se reproduire peuvent être enregistrés dans l'IRF. Des chercheurs des Pays-Bas ont réussi à créer la première balise d'IRF du monde porteuse de virus. Cette réalisation annonce peut-être un nouveau vecteur d'infection qui est dangereux.

Si les balises d'IRF réussissent à contaminer les serveurs dorsaux et que, à leur tour, ces serveurs reproduisent leurs données dans le réseau interne, les logiciels malveillants pourraient se propager très vite. Les portes dissimulées pourraient aussi s'ouvrir, ce qui permettrait l'accès à des serveurs qu'on croyait à l'abri de tout risque. Même sans les communications dorsales, ou l'écriture miroir des serveurs, la circulation des balises d'IRF infectées dans le monde entier pourrait causer des dégâts similaires⁶¹. Certains aéroports envisagent déjà de rehausser leur infrastructure de manutention des bagages au moyen de la technologie IRF. L'infection de plusieurs grands aéroports pourrait causer de graves problèmes. Ce genre d'attaques ne se limiterait pas non plus aux aéroports et aux entrepôts. L'épicerie locale qui utilise l'IRF et le vétérinaire qui fait le balayage d'une puce IRF infectée d'un animal familier pourraient eux aussi avoir des problèmes après avoir été exposés aux logiciels malveillants⁶².

La recherche dans ce domaine en est seulement à l'étape de la validation de principe, et la technologie IRF est loin d'être aussi omniprésente que les experts prétendent qu'elle pourrait le devenir. Cela pourrait

prendre quelque temps, mais les maliciels touchant l'IRF pourraient bien refaire surface dans un avenir prochain en tant que menace sérieuse.

5 Conclusion

Le paysage des logiciels malveillants est en constante évolution. Au cours des deux ou trois dernières années, un changement de tactiques s'est opéré dans le monde des maliciels, et cette tendance au changement continuera dans l'avenir. Les attaques continuent de faire état de complexité et d'organisation à des niveaux croissants. Des éléments criminels organisés s'y impliquent de plus en plus; l'argent et les menaces de violence commencent à faire partie du monde des maliciels⁶³. Les créateurs de logiciels malveillants comprennent de plus en plus les moyens illicites de tirer profit d'Internet. Beaucoup d'efforts devront être déployés pour suivre le rythme de ces menaces nouvelles qui font jour.

Puisque les menaces mentionnées dans la présente publication peuvent être combinées stratégiquement à d'autres méthodes d'attaque, comme l'ingénierie sociale, il est évident que la sensibilisation des utilisateurs est très importante. Il faudra poursuivre la recherche et continuer à agir avec prudence afin de mieux comprendre ces menaces, et le présent document servira de bon point de départ. Entre-temps, les logiciels malveillants continuent de s'attaquer aux systèmes qui résistent le moins. Il faut installer des programmes antivirus et des pare-feu et les tenir à jour. Les utilisateurs doivent faire preuve d'une prudence constante lorsqu'ils sont en ligne, et les incidents de malveillance et de nature criminelle doivent être communiqués aux organismes locaux d'application de la loi. Enfin, les mises en garde émanant des fournisseurs et des centres gouvernementaux, tels que le Centre canadien de réponse aux incidents cybernétiques (CCRIC), devraient être prises en compte. Avoir le plus possible de connaissances et de renseignements sur les systèmes exploités, c'est l'une des meilleures façons de contrer ces nouvelles menaces.

6 Glossaire⁶⁴

Attaque au jour zéro (0 jour) – Une attaque au jour zéro en est une qui exploite une vulnérabilité pour laquelle il n'existe aucun programme de protection. En général, elle signifie aussi une attaque contre une vulnérabilité qui n'est pas encore connue du public ou même des fournisseurs de la technologie qui est touchée.

Cheval de Troie – Dans le contexte informatique, un cheval de Troie est un logiciel malveillant qui est déguisé en logiciel légitime. Le terme est dérivé de la mythologie classique.

Cross-Site Scripting (XSS) – Un type de vulnérabilité en matière de sécurité informatique qu'on trouve typiquement dans les applications Web et qui peut être utilisée par un pirate informatique afin de compromettre la politique d'origine des langages de script côté client.

Générateur de virus – C'est un programme conçu pour permettre à un utilisateur qui a peu ou pas de compétences en programmation de créer un virus ou un ver et de le lancer dans Internet.

Inondeur – Un inondeur, est une personne qui envoie des pourriels. Inonder, c'est envoyer des courriels non sollicités en vrac à un grand nombre de destinataires.

Logiciel robot – Ce terme fait partie du langage courant d'Internet et désigne un agent logiciel. Les logiciels robots les plus courants sont ceux qui sont installés à des fins malveillantes, à l'insu du propriétaire de l'ordinateur.

Mystification quant au contenu – Un autre type de mystification, c'est le « Web Spoofing » (mystification de pages Web). Il s'agit d'une attaque qui reproduit une page Web légitime, comme celle d'une banque, sur un autre serveur, celui du pirate informatique, dans « son aspect et sa convivialité ». L'intention de la personne qui en est responsable est de faire croire à l'utilisateur qu'il est branché à un site de confiance et de récolter, par exemple, des noms d'utilisateurs et des mots de passe.

Pirate informatique – En matière de sécurité informatique, un pirate est une personne qui est capable d'exploiter un système ou d'y avoir un accès non autorisé au moyen d'une compétence ou d'une tactique. On retrouve parfois les termes synonymes « chapeau noir » et « casseur ».

Poste-à-poste – Un réseau informatique poste à poste est un réseau qui compte principalement sur la puissance de calcul et la largeur de bande des membres du réseau, plutôt que de se limiter à un nombre relativement restreint de serveurs. Les réseaux poste à poste sont typiquement utilisés pour les nœuds de connexion, en grande partie au moyen de connexions ad hoc.

Réseau de zombies – Ce terme du jargon informatique signifie une collection de logiciels robots qui s'exécutent de façon autonome. Le terme « réseau de zombies » peut être utilisé pour désigner n'importe quel groupe de logiciels robots, comme les robots conversation en ligne (IRC), mais il est généralement utilisé pour désigner un groupe d'appareils compromis qui exécutent des programmes (qu'on appelle normalement des vers, des chevaux de Troie ou des portes arrière) dans le cadre d'une infrastructure commune de commande et de contrôle.

Rootkit – Un « rootkit » est un ensemble d'outils logiciels utilisés souvent par un tiers (d'habitude un intrus) après que celui-ci a eu accès à un système informatique. Ces outils sont destinés à dissimuler des processus qui s'exécutent, des fichiers ou des données de système, ce qui permet à l'intrus de maintenir son accès à l'ordinateur à l'insu de l'utilisateur.

Tête de réseau de zombies – « Tête de réseau de zombies » est un terme généralement reconnu pour désigner la personne à la tête de vastes réseaux de systèmes compromis qui forment des réseaux de zombies.

Vecteur de propagation – Au sens de l'informatique, en particulier de logiciels malveillants comme les virus et les vers, un vecteur est une méthode utilisée par le logiciel pour se propager et infecter un ordinateur. Ce sens est similaire à celui qu'on lui donne en biologie, et il en dérive d'ailleurs. Voici des exemples de vecteurs courants :

- surcharge de la mémoire tampon;
- courriel en HTML avec JavaScript ou autres améliorations de scripts;
- défauts dans les protocoles de réseautage – c'est de cette manière que le ver Blaster a pu se propager.

Ver – Un ver informatique est un programme autoreproducteur. Il est autonome et n'a pas besoin de s'inscrire dans un autre programme pour se propager. Il est souvent conçu pour exploiter les capacités de transmission de fichiers que possèdent beaucoup d'ordinateurs.

Zombie – Un ordinateur zombie, ou simplement « zombie », est un ordinateur branché à Internet qui a été compromis par un pirate informatique, un virus ou un cheval de Troie.

- 1 Robert Richardson *et al.*, *CSI/FBI Computer Crime and Security Survey* (San Francisco: Computer Security Institute, 2005) at 13, online: Computer Security Institute <http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf>.
- 2 The original idea for this report was born out of the paper *Malware – future trends*, written by Dancho Danchev. His complete paper can be found here: <http://www.packetstormsecurity.org/papers/general/malware-trends.pdf>.
- 3 Ryan Naraine, “Researcher: WMF Exploit Sold Underground for \$4,000,” (2 February 2006) online: eWeek.com <<http://www.eweek.com/article2/0,1895,1918198,00.asp>>. [WMF]
- 4 Yury Mashevsky, “Watershed in malicious code evolution,” (29 July 2005) online: Viruslist.com <<http://www.viruslist.com/en/analysis?pubid=167798878>>. [Watershed]
- 5 Dr. Steven Furnell & Dr. Jeremy Ward, “The True Computer Parasite,” (1 June 2005) online: SecurityFocus <<http://www.securityfocus.com/infocus/1838>>.
- 6 National Infrastructure Security Coordination Center, “The Quarterly – The growing online marketplace,” (February 2005) at 4, online: NISCC <<http://www.niscc.gov.uk/niscc/docs/re-20050728-00635.pdf?lang=en>>.
- 7 National Infrastructure Security Coordination Center, “Targeted Trojan E-mail Attacks,” (16 June 2005) at 4, online: NISCC <<http://www.niscc.gov.uk/niscc/docs/tea.pdf>>.
- 8 *Watershed*, *supra* note 4.
- 9 Tom Sanders, “Cops smash 100,000 node botnet,” (10 October 2005) online: Vnunet.com <<http://www.vnunet.com/vnunet/news/2143475/dutch-police-foil-100-node>>.
- 10 Alexander Gostev, “Malware Evolution: January - March 2005,” (18 April 2005) online: Viruslist.com <<http://www.viruslist.com/en/analysis?pubid=162454316>>.
- 11 David Emm, “Rise of the ‘business worm’?,” (19 August 2005) online: Viruslist.com <<http://www.viruslist.com/en/analysis?pubid=168953110>>.
- 12 U.S. Department of Energy – Computer Incident Advisory Capability, “P-256 Targeted Attacks,” (18 July 2005) online: US DoE – CIAC <<http://www.ciac.org/ciac/bulletins/p-256.shtml>>.
- 13 David Sancho, “The Future of Bot Worms,” (18 August 2005) at 1, online: Trend Micro <<http://www.trendmicro.com/en/offers/global/outbreak-aug18-wp.htm>>.
- 14 Dean Turner *et al.*, *Symantec Internet Security Threat Report – Trends for July 05-December 05* (Cupertino, California: Symantec, 2006) at 55-57. [Symantec]
- 15 *Watershed*, *supra* note 4.
- 16 *Watershed*, *supra* note 4.
- 17 *Symantec*, *supra* note 14 at 14.
- 18 Dancho Danchev, “Malware – future trends,” (9 January 2006) at 3, online: PacketStorm Security <<http://www.packetstormsecurity.org/papers/general/malware-trends.pdf>>. [Malware]
- 19 *Ibid.* at 3.
- 20 Infectionvectors, “Agobot and the ‘Kit’chen Sink,” (July 2004) at 4-5, online: Infectionvectors.com <http://www.infectionvectors.com/vectors/Agobot_&_the_Kit-chen_Sink.pdf>.
- 21 *Symantec*, *supra* note 14 at 16.
- 22 *Symantec*, *supra* note 14 at 75.
- 23 *Malware*, *supra* note 19 at 17.
- 24 *Symantec*, *supra* note 14 at 72.
- 25 *Malware*, *supra* note 19 at 18.
- 26 *Watershed*, *supra* note 4.
- 27 Sharp Ideas LLC, “Pod Slurping,” (2005) online: Sharp Ideas LLC <http://www.sharp-ideas.net/pod_slurping.php>.
- 28 Trend Micro, “SYMBOS_CARDTRP.D,” online: Trend Micro <<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=SYMBOS%5FCARDTRP%2ED&VSect=T>>.
- 29 Chris Davis & Aaron Higbee, “DC Phone Home,” (31 July 2002) online: Black Hat <<http://www.blackhat.com/presentations/bh-usa-02/higbee-davis/higbeedavis-bh-us-02-phone.ppt>>.
- 30 iDefense, “Rootkits and Other Concealment Techniques in Malcode,” (17 February 2006) at 19, online: iDefense <<http://www.iddefense.com/intelligence/researchpapers.php>>.
- 31 *Symantec*, *supra* note 14 at 20.
- 32 Alisa, “Subversive SubVirt,” (16 March 2006) online: Viruslist.com <<http://www.viruslist.com/en/weblog?weblogid=182153387>>.

-
- 33 Robert Lemos, "Researchers: Rootkits headed for BIOS," (26 January 2006) online: SecurityFocus <<http://www.securityfocus.com/news/11372>>.
- 34 *Symantec*, *supra* note 14 at 12.
- 35 Paul Stamp *et al.*, "Increasing Organized Crime Involvement Means More Targeted Attacks," (2 August 2005) at 2, online: SEC Consult <<http://www.sec-consult.com/fileadmin/Newsletters/newsletter092005.pdf>>.
- 36 *Symantec*, *supra* note 14 at 12.
- 37 Adam Young & Moti Young, "Cryptovirology: Extortion-Based Security Threats and Countermeasures," (6 May 1996) online: VX Heavens <<http://vx.netlux.org/lib/ayo00.html>>.
- 38 "AIDS (trojan horse)," online: Wikipedia <http://en.wikipedia.org/wiki/AIDS_%28trojan_horse%29>.
- 39 LURHQ Threat Intelligence Group, "Cryzip Ransomware Trojan Analysis," (11 March 2006) online: LURHQ <<http://www.lurhq.com/cryzip.html>>.
- 40 Daniele Micci-Barreca, "Unawed by Fraud," (September 2003) online: Security Management Online <<http://www.securitymanagement.com/library/001490.html>>.
- 41 MaxMind, "MaxMind GeoIP® City Database," online: MaxMind <<http://www.maxmind.com/app/city>>.
- 42 *Malware*, *supra* note 19 at 18.
- 43 John Leyden, "Slobodan Trojan poses as murder pics," (15 March 2006) online: The Register <http://www.theregister.co.uk/2006/03/15/slobodan_trojan>.
- 44 *Malware*, *supra* note 19 at 18.
- 45 *Symantec*, *supra* note 14 at 17.
- 46 Massimiliano Romano *et al.*, "Robot Wars – How Botnets Work," (20 October 2005) online: WindowsSecurity.com <<http://www.windowsecurity.com/articles/Robot-Wars-How-Botnets-Work.html>>. [*Robot*]
- 47 David Sancho, "Rootkits: The new wave of invisible malware is here," (2005) at 2, online: Trend Micro <<http://www.trendmicro.com/NR/rdonlyres/388874B6-C27C-4354-9078-42771EABEBB1/18503/rootkitwp.pdf>>.
- 48 *Malware*, *supra* note 19 at 18-19.
- 49 *Watershed*, *supra* note 4.
- 50 *Robot*, *supra* note 47.
- 51 Paul F. Roberts, "Botnet Uses BitTorrent to Push Movie Files," (21 December 2005) online: eWeek.com <<http://www.eweek.com/article2/0,1759,1904429,00.asp>>.
- 52 *Symantec*, *supra* note 14 at 56.
- 53 *WMF*, *supra* note 3.
- 54 *Malware*, *supra* note 19 at 21.
- 55 *Symantec*, *supra* note 14 at 22.
- 56 Web Application Security Consortium, "Content Spoofing," online: WASC <http://www.webappsec.org/projects/threat/classes/content_spoofing.shtml>.
- 57 "Cross site scripting," online: Wikipedia <http://en.wikipedia.org/wiki/Cross_site_scripting>.
- 58 *Malware*, *supra* note 19 at 24.
- 59 *Symantec*, *supra* note 14 at 22.
- 60 Melanie R. Rieback *et al.*, "Is Your Cat Infected with a Computer Virus?," (March 2006) at 3, online: Vrije Universiteit Amsterdam <<http://www.rfidvirus.org/papers/percom.06.pdf>>.
- 61 *Ibid.* at 4.
- 62 "RFID Viruses and Worms," online: Vrije Universiteit Amsterdam <<http://www.rfidvirus.org>>.
- 63 Phil Williams, "Organized Crime and Cyber-Crime: Implications for Business," (2002) at 2, online: CERT.org <<http://www.cert.org/archive/pdf/cybercrime-business.pdf>>.
- 64 The definitions for the terms found in the glossary are originally found in the Wikipedia. <<http://www.wikipedia.org>>.