German
Data
Security

G Data Whitepaper 2009

Comment les codes nuisibles parviennent-ils aux ordinateurs d'entreprise ?

Ralf Benzmüller, Werner Klier & Jérôme Granger
G Data Security Labs

Go safe. **Go safer. G Data.**

Table des matières

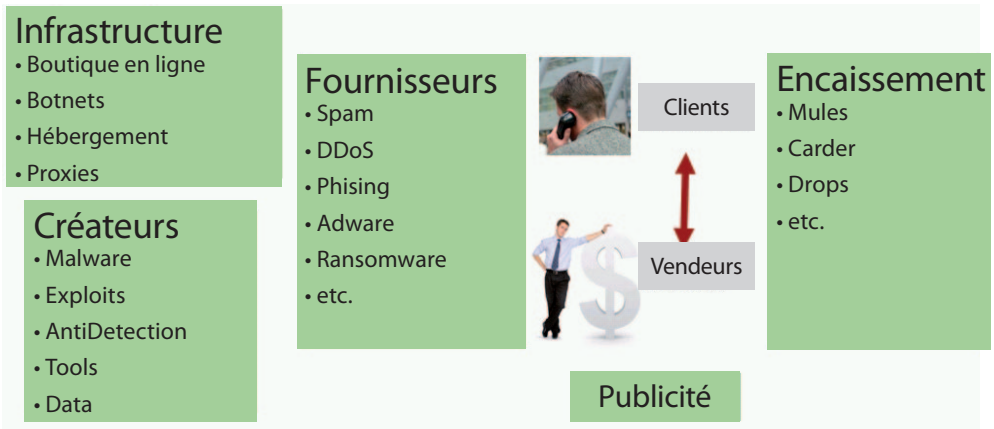
1. Les malwares, base de la cyberéconomie souterraine

Dans le monde numérique clandestin, une véritable économie parallèle s'est créée au sein de laquelle des structures rigoureusement organisées mettent au point, perfectionnent et diffusent des logiciels malveillants professionnels à des fins économiques.

Sur les places de marché cybercriminelles, tout se vend et tout s'achète, de la prestation de services aux marchandises. Sur ces plateformes commerciales, il est ainsi possible de trouver des informations sur les nouvelles failles de sécurité détectées ainsi que des logiciels malveillants adaptés. Leurs auteurs vont même jusqu'à garantir le fonctionnement de l'outil et assure un suivi technique en fournissant gratuitement aux acheteurs des versions modifiées pendant la période de garantie.

Des armées d'ordinateurs infectés, les réseaux zombies, sont également louées à l'heure ou à la journée pour l'exécution de campagnes de spams ou d'attaques ciblées contre des sites Web ou serveurs de messagerie. Le blanchiment de l'argent, dernier maillon de la chaîne, est assuré par différents systèmes illégaux. Des entreprises fictives peuvent par exemple engager des particuliers comme « agents financiers », ces derniers mettant en retour leur compte bancaire privé à disposition pour des transactions financières.

Dans cette économie, l'entreprise est bien entendue une cible privilégiée. Toutes les informations sont recherchées, qu'elles soient stratégiques pour la revendre à la concurrence, ou techniques pour pouvoir utiliser l'infrastructure du réseau à des fins criminelles.



Ill. 1 : Les différents piliers économiques de la criminalité électronique

Comme le montre l'illustration 1, l'économie de la criminalité électronique est finalement très proche de celle de l'économie légale. De l'infrastructure commerciale, jusqu'à la vente, tous les maillons de la chaîne sont présents. Seule l'étape de l'encaissement diffère. Les acteurs de ce marché parallèle doivent trouver des systèmes de blanchiment afin de convertir leurs revenus illégaux en argent propre.

2. Les Méthodes d'infections

Les logiciels malveillants peuvent infiltrer les ordinateurs PC de l'entreprise d'une multitude de manières. Dans certains cas, il suffit de connecter l'ordinateur à Internet ou à un réseau local. Cependant, les courriers électroniques, les bourses d'échanges, les messages instantanés et les supports de données peuvent également inclure des codes malveillants. Les sites Web préparés, qui téléchargent directement le fichier ou infectent l'ordinateur en arrière-plan (Drive By Download), sont actuellement les plus dangereux.

2.1 Une connexion suffit

Les innombrables vers qui circulent en permanence et de manière autonome sur Internet constituent une menace constante pour les ordinateurs connectés à Internet. Ils génèrent sans arrêt des adresses IP aléatoires et déterminent si les ordinateurs correspondants sont sensibles aux failles de sécurité. La sélection d'adresses IP est souvent limitée. Ainsi, seules certaines parties du réseau (un fournisseur Internet ou une région en particulier, par exemple) sont sélectionnées. Les failles de sécurité utilisées évoluent au fil du temps. Des failles de sécurité résolues de longue date sont ainsi encore étudiées, comme celles de Blaster (2003) et de Sasser (2004). Les cibles des attaques les plus fréquentes sont répertoriées dans la liste suivante:

- Plug'n'Play (MS05-039) via TCP/445, TCP/139
- RPC-DCOM (MS03-026/MS03-039) via TCP/135, TCP/445, TCP/1025
- LSASS (MS04-011) via TCP/445
- MySQL via TCP/3306
- Arkeia via TCP/617
- Veritas via TCP/6101
- Veritas via TCP/10000
- WINS via TCP/42
- Arcserve via TCP/41523
- NetBackup via TCP/13701
- Workstation Service (MS03-049) via TCP/135, TCP/445
- WebDaV via TCP/80
- DameWare via TCP/6129
- Porte dérobée MyDoom via TCP/3127
- Porte dérobée Bagle via TCP/2745
- IIS 5.x SSL PCT (MS04-011) via TCP/443
- Comptes avec des mots de passe banals (connexion via TCP/139 ou TCP/445)
- Serveurs MSSQL avec mot de passe banal (par exemple, compte SA avec mot de passe vide) via TCP/1433

Des études récentes montrent que les ordinateurs Windows sont attaqués une fois toutes les 38 secondes en moyenne. Comme bien des administrateurs système en ont déjà fait l'expérience, des ordinateurs réparés peuvent être de nouveau attaqués en l'espace de quelques secondes, pendant le téléchargement du correctif. Une rapidité qui vient du fait que la création de codes « exploit » s'est professionnalisée. Les codes « exploit » des failles de sécurité apparaissent souvent seulement quelques jours après le premier compte-rendu. Le nombre de codes « exploit » utilisés par des logiciels malveillants (Zero Day Exploits) est en constante augmentation. Le dernier exemple est le ver Conficker qui, parallèlement à la diffusion automatique, utilise les activations locales avec mot de passe inefficace et le mécanisme de démarrage automatique des supports de données USB pour se propager. Ce type d'attaques fonctionne sans l'aide de l'utilisateur de l'ordinateur et le plus souvent, à son insu. Un pare-feu correctement configuré ou un routeur permet de se protéger contre de telles attaques.

2.2 Par site Web

Les sites Web représentent actuellement la principale porte d'entrée des nouveaux programmes nuisibles. Ils utilisent une faille structurelle dans le fonctionnement des outils d'analyse antivirus. Les outils d'analyse antivirus vérifient les fichiers lorsqu'un composant du système souhaite y accéder (OnAccess) ou à la demande (OnDemand). La vérification de l'antivirus a donc lieu alors que le code nuisible est déjà présent en tant que fichier. Si les données du site Web sont transmises au navigateur par le biais du protocole HTTP, les codes HTML et les commandes de script inclus sont interprétés et exécutés dans la mémoire de travail du navigateur. Le navigateur détermine ensuite si le contenu peut être enregistré sur le disque dur. Il est possible que l'alarme de l'outil d'analyse antivirus se déclenche alors. Les codes nuisibles sont cependant déjà exécutés. Pour que les outils d'analyse antivirus protègent efficacement des sites Web nuisibles, le contenu du flux de données HTPP doit être vérifié avant qu'il parvienne au navigateur, c'est le scan HTTP.

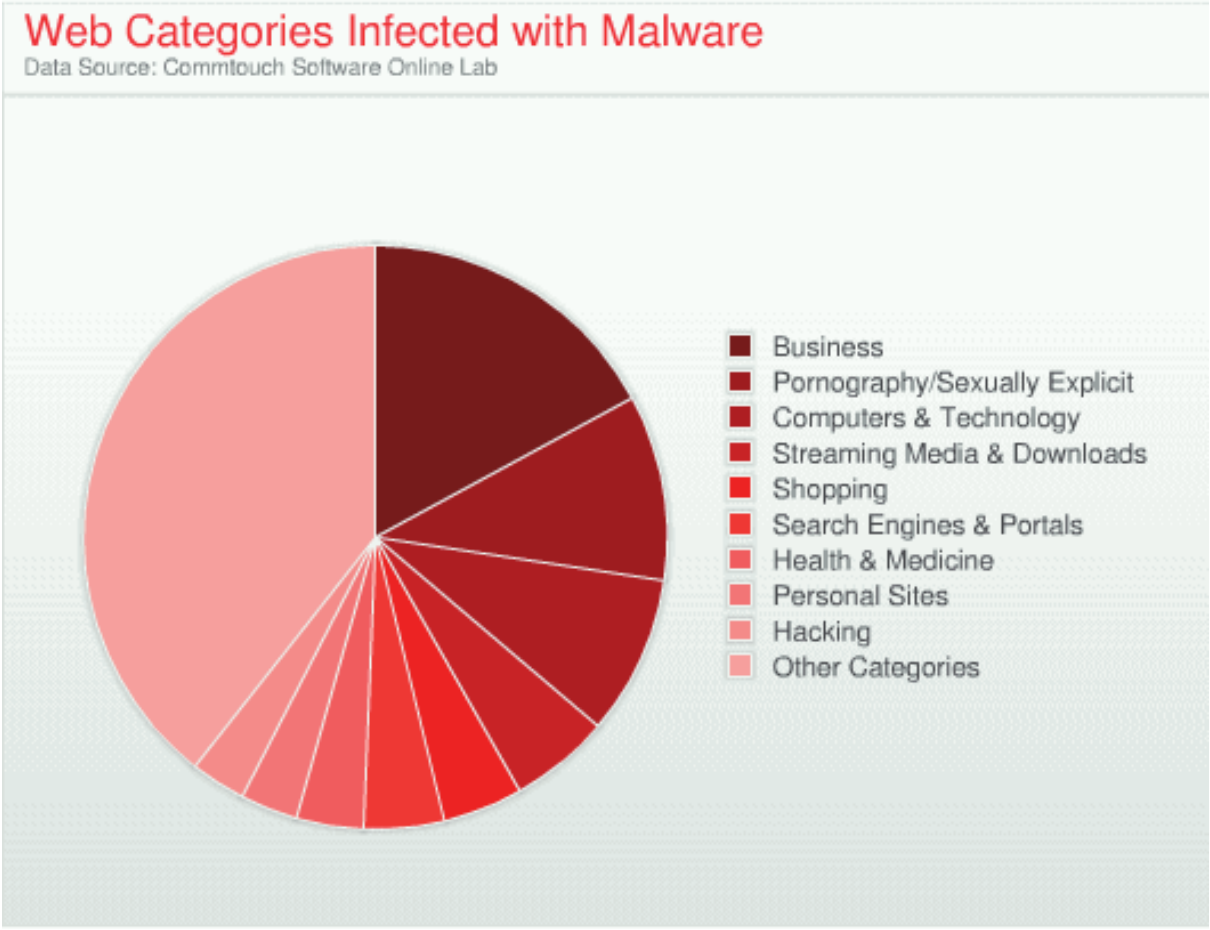
Il existe différentes techniques d'attaque. Celles appelées « Drive By Download » sont à l'heure actuelle en recrudescence. Tandis que les téléchargements doivent être demandés par le visiteur du site Web, les Drive By Download ont lieu lors d'une simple visite d'un site.

Le Drive By Download

Lors de la navigation, des scripts insérés dans la page infectée déterminent le navigateur et le système d'exploitation utilisés par l'ordinateur du visiteur. L'adresse IP de la machine est aussi relevée. Les résultats sont ensuite stockés sur un ordinateur serveur contrôlé par le diffuseur du logiciel malveillant. Un code nuisible va alors rechercher les failles de sécurité au niveau du navigateur et de ses composants. Si la recherche est positive, le code nuisible qui utilise la faille de sécurité en question est transféré sur l'ordinateur et en prend le contrôle. Ces codes nuisibles sont appelés des codes « exploits ». La plupart des codes «exploits » en circulation sont conçus pour les ordinateurs Windows équipés de l'application Internet Explorer (l'association la plus utilisée). Les failles de sécurité de Firefox, Opera et Safari sont cependant également utilisées. Des outils tels que MPack, IcePack ou FirePack sont utilisés afin de garantir l'installation correcte des scripts. Les auteurs de logiciels malveillants utilisent actuellement le plus souvent les failles de sécurité suivantes :

- CVE 2007-0071 Adobe Flash
- CVE 2008-1309 RealPlayer

- ourgame_GLIEDown2 Internet Explorer
- CVE 2006-0003 MS06-01, MDAC
- CVE 2007-5601 RealPlayer



Ill. 2 : les pages professionnelles, premières cibles des attaques par Drive by Download

Les fausses pages web

Une fois le serveur prêt, le diffuseur de logiciels malveillants doit encore attirer le visiteur sur sa page. Cela a lieu par le biais de messages indésirables qui attirent sur la page en évoquant un contenu intéressant, des offres spéciales ou des gains de loterie. Les demandes au niveau de moteurs de recherche connus, tels que Google, Yahoo et Bing, sont également de plus en plus souvent manipulées de manière à ce que les sites Web nuisibles apparaissent parmi les premiers résultats. Une erreur de frappe dans la saisie du lien du navigateur peut également reconduire vers des sites nuisibles. Exemples : « mircosoft.com », « goggle.com » ou « mcaffe.de », il suffit d'intervertir deux lettres pour être dirigé vers une mauvaise adresse infectée.

L'intégration du code dans des sites officiels

Il est cependant beaucoup plus efficace d'intégrer le code nuisible aux pages Web d'un domaine connu. Le trafic est garanti et l'impact est donc plus grand. Mais il faut avant tout prendre le contrôle du serveur Web. Il existe pour cela des outils qui, via des attaques par dictionnaire, tentent de deviner le mot de passe d'accès de l'administrateur du serveur Web.

Les failles de sécurité de logiciels Web courants, tels que les systèmes de gestion du contenu, les logiciels de forums et blogs et les outils d'administration, sont également utilisées pour prendre le contrôle du serveur Web. Dans la majorité des cas, ces attaques ne se limitent pas à quelques serveurs Web, elles sont exécutées de manière massive et automatisée.

La prise de contrôle du serveur Web effectuée, une ligne permettant de charger le code nuisible à partir d'un autre serveur (via IFRAME ou SCRIPT, par exemple) est ajoutée à l'aide des packs de codes « exploit » web.

Une autre possibilité consiste à modifier les publicités des pages Web. Les bannières publicitaires étant généralement gérées par des centrales publicitaires, l'administrateur du site n'a souvent aucune influence sur leur contenu. Ces pages sont donc généralement mises à jour via IFRAME. Ces liens vers les serveurs peuvent être détournés au profit du pirate. Les scripts nuisibles créés à l'aide de MPack ou d'outils similaires sont particulièrement bien dissimulés et chiffrés (il est possible de créer des codes nuisibles polymorphes avec les langages de script). Il est ainsi possible d'intégrer des codes nuisibles à des sites Web légitimes. Environ 80 % des infections Drive By ont lieu sur des sites Web légitimes. L'intégration de codes dans les liens vers les forums, blogs ou courriers électroniques est aussi possible. L'interactivité d'Internet offre une multitude de forums de discussion et de sites Wiki auxquels le participant peut apporter sa contribution et y déposer des fichiers. Un auteur Wikipedia est ainsi parvenu à insérer un lien vers un cheval de Troie, sous couvert d'un outil de suppression du ver Blaster.

Le Cross Site Scripting

L'intégration d'un code nuisible sur un serveur n'est pas indispensable. Le lien vers le site Web peut inclure directement le code nuisible, qui est ensuite exécuté sur la page cible. Cette attaque est appelée Cross Site Scripting (XSS). Les attaques XSS sont possibles lorsque la saisie d'un utilisateur est de nouveau affichée sur une page ultérieure et que l'absence de contenu exécutable au niveau de la saisie n'est pas vérifiée. Prenons l'exemple du nom d'un formulaire qui est de nouveau affiché lors de la commande suivante. Si le pirate saisit un code JavaScript à la place de son nom, le code est, dans la mesure où il n'est pas filtré, exécuté par le navigateur. Un exemple d'attaque Cross Site Scripting : un formulaire demande la saisie d'un nom. Le pirate saisit le code suivant à la place de son nom :

```
<SCRIPT>alert(„You're pwned")</SCRIPT>.
```

Une fois le formulaire envoyé, le code n'est pas affiché, mais exécuté sur la page suivante. Dans le cas présent, un message d'avertissement s'affiche. Les véritables attaques incluent un code dangereux.

Le code nuisible peut être directement intégré au lien vers la page activée, même

lorsque la saisie du formulaire est filtrée. Exemple :

```
http://www.myserver.dom/site.php?name=<SCRIPT>alert(„You're pwned")</
SCRIPT>.
```

Un tel lien peut se cacher dans le texte de n'importe quel forum ou blog. L'attaque est encore plus perfide lorsque de tels liens XSS apparaissent dans les résultats de recherche de Google. Les auteurs de logiciels malveillants optimisent les entrées de blog corrompues pour le moteur de recherche de Google. Grâce à quelques astuces de dissimulation, ce phénomène est de plus

en plus fréquent, même si Google tente de détecter de tels liens XSS et de les supprimer des résultats de recherche. La situation est comparable avec les nombreuses possibilités nouvelles offertes par le Web 2.0. Les personnes qui, en raison de la menace, jugent utile d'interdire le contenu actif ou les langages de script de leur navigateur renoncent également aux possibilités du Web 2.0. Un grand nombre de ces nouvelles fonctions présentent également des risques d'utilisation abusive et augmentent le nombre de failles de sécurité possibles. À la fin de l'année 2005, le ver XSS de Samy est parvenu, par le biais d'une attaque Cross Site Scripting (XSS), à se créer plus d'un million d'amis sur MySpace en l'espace de 18 heures. Le danger du Cross Site Scripting reste sous-estimé, car tous les sites Web peuvent contenir des codes nuisibles.

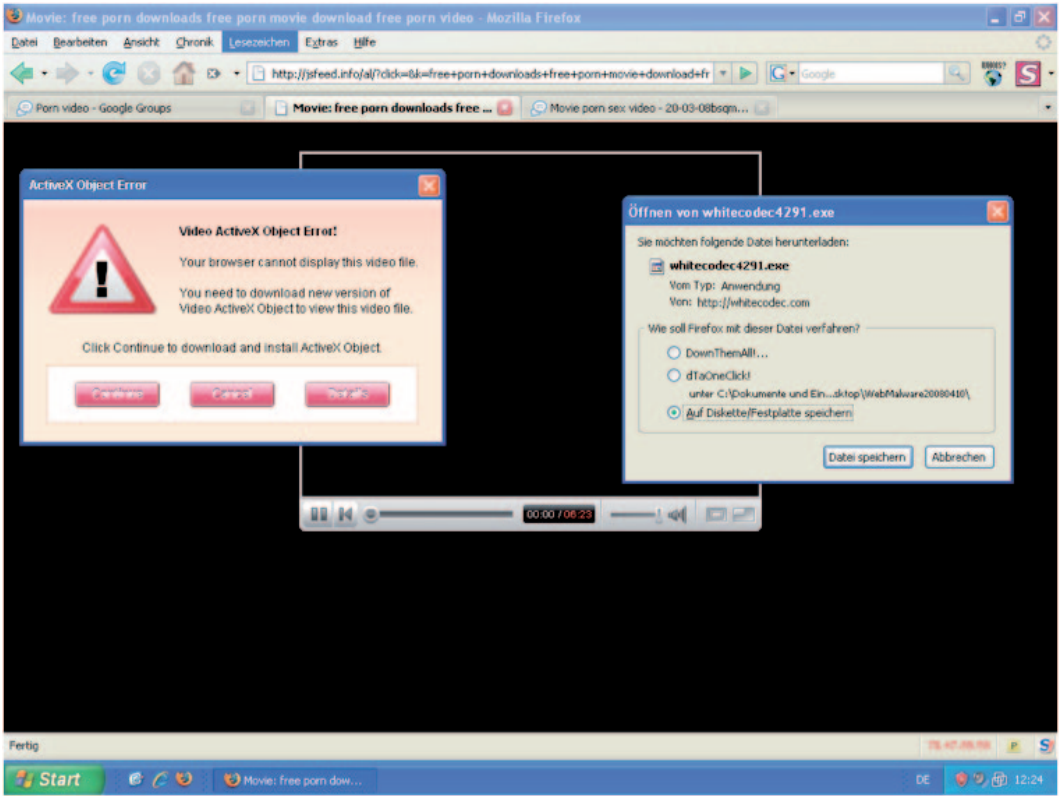
Les attaques psychologiques

Pas toujours techniques, certaines méthodes font davantage appel à la psychologie.

La mode est au scareware. Ces logiciels basés sur la peur font croire à la victime, par le biais de faux messages d'avertissement, que le système est infecté. Pour enrayer l'infection, la victime doit alors acheter la version complète de ce soi-disant produit de sécurité. En plus de payer environ 50 dollars pour ce faux outil d'analyse, les numéros de carte sont volés et réutilisés pour d'autres achats.

Ill. 3 : le site Web d'un logiciel basé sur la peur demande les références de carte de crédit de la victime

Une autre astuce consiste à attirer la victime sur un site Web où se trouve soi-disant une vidéo. Il peut s'agir d'un contenu érotique ou d'une référence à un événement d'actualité (catastrophe naturelle, accident d'avion, élection présidentielle, événement sportif). Pour visionner la vidéo vantée, le visiteur doit alors installer un codec vidéo spécial ou une version plus récente du lecteur Flash. Il s'agit bien sûr d'un logiciel malveillant.



Ill. 4 : un prétendu site Web de vidéos qui propose de télécharger un codec infecté

2.3 Par courrier électronique

Très utilisés dans une entreprise, les conversations et l'échange de documents par e-mail sont des facteurs de diffusion majeurs de dangers. Très à la mode dans les années 2000, la propagation de programmes nuisibles par ce biais est encore d'actualité. Bien sûr, les

Loveletter, Melissa, Sobig ou Netsky, qui avaient mis à genoux les serveurs de messagerie de la planète, sont de plus en plus rares et ne sont plus utilisés dans la diffusion de vers. Sober, Nyxem (2004) et Warezov (2007) sont les derniers vers transmis par courrier électronique. Depuis, les vagues d'infection sont plus limitées, dans la diffusion, le temps et l'espace. Contrairement aux infections automatisées des vers Internet, les vers des courriers électroniques ne sont dangereux que si le destinataire ouvre le fichier en pièce jointe. La simple réception du courrier nuisible ne présente que très peu de danger. Dans seulement quelques rares cas, l'affichage du courrier électronique au niveau du client peut être un vecteur d'infection (Bubbleboy et Klez, par exemple). Même si les vers de courriers électroniques nécessitent l'intervention du destinataire, une ouverture malencontreuse est toujours possible. De multiples astuces poussent quelques fois les utilisateurs à ouvrir les pièces jointes. Une situation qui prend tout son sens en entreprise. Si dans le cadre personnel, il est aisé de faire le tri dans ses mails (les noms d'inconnus étant rapidement éliminés), en entreprise la pratique est plus délicate. Clients et contacts divers, utilisant quelques fois des langues différentes, peuvent être amenés à communiquer avec un salarié. Le risque de cliquer sur un fichier malveillant apparemment sain est alors important.

Les fichiers exécutables des courriers électroniques étant désormais filtrés (au niveau de la passerelle ou du client) et les utilisateurs des messageries électroniques mieux conscients des dangers, les auteurs de logiciels malveillants envoient désormais des liens vers des fichiers

stockés sur Internet. Ces courriers électroniques ne sont donc pas considérés comme nuisibles par les antivirus. Seul un filtre antispam peut les détecter. Pour pousser la victime à exécuter le fichier ou à activer le site Web les méthodes ne manquent pas. Propositions commerciales, sites soi-disant intéressants, visualisation du bulletin de paie en ligne… tout est utilisé pour tromper le salarié.

Jordan et Goudey (2005) ont identifié les douze facteurs psychiques suivants comme bases des vers les plus couronnés de succès entre 2001 et 2004. Une étude ancienne, mais qui est malheureusement toujours d'actualité :

- Inexpérience (inexperience)
- Curiosité (curiosity)
- Avidité (greed)
- Manque de confiance en soi (diffidence)
- Politesse (courtesy)
- Amour de soi (self-love)
- Crédulité (credulity)
- Désir (desire)
- Envie et amour (lust)
- Menace (dread)
- Réciprocité (reciprocity)
- Amitié (friendliness)

Un autre chercheur, M. Braverman complète la liste :

- Conversation générale (generic conversation) : Expressions courtes, telles que « Cool », etc.
- Avertissements relatifs à des virus et correctifs logiciels
- Logiciels malveillants détectés sur l'ordinateur PC
- Message de vérification antivirus à la fin du courrier
- Informations ou messages relatifs à des comptes : le cheval de Troie Telekom, par exemple, qui se présente comme une facture téléphonique excessive
- Messages d'erreur relatifs à la distribution du courrier
- Attraction physique (Physical attraction) (chevauchement avec le point Envie et amour de la liste de Jordan et Goudey)
- Accusations (Accusatory) : par exemple, le cheval de Troie BKA qui prétend avoir détecté des fichiers illégaux
- Événements actuels
- Free stuff : certaines personnes se laissent totalement duper dès que quelque chose de gratuit leur est proposé

2.4 Par message instantané

De plus en plus utilisée dans les entreprises, la messagerie instantanée est le nouveau casse-tête des administrateurs réseau. La collecte n'étant pas centralisée comme celle du mail avec les serveurs de messagerie, le filtrage en amont du poste client n'est pas possible. Il faut donc confier le travail à l'antivirus local. Mais comme sur l'e-mail, la plupart des vers de messages instantanés optent pour des liens de téléchargement insérés dans les messages. Ces attaques sont là encore souvent basées sur l'ingénierie sociale. Bien souvent, vous êtes invité à vous rendre sur un site amusant ou étonnant… Certains vers de messages instantanés possèdent des moteurs de chats et sont en mesure de mener de brèves conversations. Si vous utilisez la messagerie instantanée dans votre entreprise, il est impératif d'opter pour un client capable de vérifier les fichiers entrants. Certains clients offrent également la possibilité d'activer un outil d'analyse antivirus par le biais d'une ligne de commande.

2.5 Par réseaux P2P

Les réseaux P2P sont un autre casse-tête pour les entreprises. Étant pénalement impliquées en cas de téléchargement illégal de fichiers soumis au droit d'auteur par un salarié, elles se doivent d'en limiter l'accès. Si la pratique est aisée dans les grandes entreprises, les administrateurs réseau étant au fait des ports à bloquer sur les passerelles, elle est beaucoup moins évidente pour les plus petites structures. Au-delà des implications juridiques, les réseaux P2P représentent un risque majeur pour l'intégrité des réseaux de l'entreprise. Une étude menée par G Data montre que sur le top 20 des jeux les plus vendus, 33 % de ces mêmes titres présents sur les réseaux P2P sont infectés. Cette étude menée sur les 1 000 premiers fichiers téléchargés, indique ainsi que plus de deux tiers des programmes nuisibles (68 %) étaient des logiciels publicitaires, 23 % étaient des chevaux de Troie et 5 % des portes dérobées. Au cours des six mois de l'étude, plus de la moitié des fichiers vérifiés provenant des bourses d'échanges P2P intégraient des codes nuisibles. La valeur a atteint un pic de plus de 65 % de fichiers infectés à la fin de l'étude.

2.6 Par support de données

Entrer dans un réseau d'entreprise peut se faire de multiples façons. L'une des méthodes les plus originales est sans doute celle qui consiste à laisser des clés USB infectées par des logiciels espions sur le parking des entreprises. Lorsque les employés connectent la clé sur leur PC de bureau pour savoir ce qui y est stocké, ils infectent alors leur ordinateur.

Des attaques permises par certains éléments techniques porteurs. Le ver Conficker, omniprésent dans les médias au début de l'année 2009, utilise notamment la fonction d'exécution automatique de Windows pour se propager par le biais des supports de données amovibles. Les vers de la famille Autorun utilisent également cette « fonction » de Windows et sont à l'origine d'une recrudescence des vers depuis le deuxième semestre 2008. Les conseils pour désactiver facilement la fonction d'exécution automatique n'ont pas abouti étant donné que cela n'était possible que via un correctif Microsoft adapté. Une lacune corrigée par Windows 7 : Microsoft a désactivé l'exécution automatique sur son nouveau système.

2.7 Via les réseaux locaux

Les vers peuvent également se propager au niveau des réseaux locaux. Certains vers se copient dans toutes les zones librement accessibles. Ils utilisent souvent des listes avec les mots de passe les plus courants. Conficker s'appuie également sur cette faille. C'est la raison pour laquelle les entreprises doivent utiliser des mots de passe sécurisés et s'assurer quotidiennement de

l'absence de codes nuisibles. Certaines variantes de Rbot et Conficker utilisent notamment les noms d'utilisateur suivants :

« ADMIN », « ADMINISTRADOR », « ADMINISTRAT », « ADMINISTRATEUR », « ADMINISTRATOR », « ADMINS », « COMPUTER », « DATABASE », « DB2 », « DBA », « DEFAULT », « GUEST », « NET », « NETWORK », « ORACLE », « OWNER », « ROOT », « STAFF », « STUDENT », « TEACHER », « USER », « VIRUS », « WWWADMIN »

et les mots de passe suivants :

« 0 », « 000 », « 007 », « 1 », « 12 », « 123 », « 1234 », « 12345 », « 123456 », « 1234567 », « 12345678 », « 123456789 », « 1234567890 », « 12345678910 », « 2000 », « 2001 », « 2002 », « 2003 », « 2004 », « ACCESS », « ACCOUNTING », « ACCOUNTS », « ADM », « ADMIN », « ADMINISTRADOR », « ADMINISTRAT », « ADMINISTRATEUR », « ADMINISTRATOR », « ADMINS », « BASD », « BACKUP », « BILL », « BITCH », « BLANK », « BOB », « BRIAN », « CHANGEME », « CHRIS », « CISCO », « COMPAQ », « COMPUTER », « CONTROL », « DATA », « DATABASE », « DATABASEPASS », « DATABASEPASSWORD », « DB1 », « DB1234 », « DB2 », « DBA », « DBPASS », « DBPASSWORD », « DEFAULT », « DELL », « DEMO », « DOMAIN », « DOMAINPASS », « DOMAINPASSWORD », « ERIC », « EXCHANGE », « FRED », « FUCK », « GEORGE », « GOD », « GUEST », « HELL », « HELLO », « HOME », « HOMEUSER », « HP », « IAN », « IBM », « INTERNET », « INTRANET », « JEN », « JOE », « JOHN », « KATE », « KATIE », « LAN », « LEE », « LINUX », « LOGIN », « LOGINPASS », « LUKE », « MAIL », « MAIN », « MARY », « MIKE », « NEIL », « NET », « NETWORK », « NOKIA », « NONE », « NULL », « OAINSTALL », « OEM », « OEMINSTALL », « OEMUSER », « OFFICE », « ORACLE », « ORAINSTALL », « OUTLOOK », « OWNER », « PASS », « PASS1234 », « PASSWD », « PASSWORD », « PASSWORD1 », « PETER », « PWD », « QAZ », « QWE », « QWERTY », « ROOT », « SA », « SAM », « SERVER », « SEX », « SIEMENS », « SLUT », « SQL », « SQLPASS », « STAFF », « STUDENT », « SUE », « SUSAN », « SYSTEM », « TEACHER », « TECHNICAL », « TEST », « UNIX », « USER », « VIRUS », « WEB », « WIN2000 », « WIN2K », « WIN98 », « WINDOWS », « WINNT », « WINPASS », « WINXP », « WWW », « WWWADMIN », « XP », « ZXC »

Les utilisateurs de votre réseau doivent renoncer à ces mots de passe et aux mots de passe similaires (y compris à leur traduction française).

3. Déroulement d'une attaque

Les attaques des cybercriminels se déroulent généralement selon un patron caractéristique.

Au cours des dernières années, de nombreux petits modules compacts et hautement spécialisés sont apparus. L'infection se déroule en plusieurs phases. Une fois le programme nuisible préparé et les victimes potentielles sélectionnées, l'attaque est lancée. Les systèmes infectés, qui se trouvent sous le contrôle du pirate, peuvent ensuite être utilisés pour quasiment toutes les activités criminelles possibles.

3.1 Préparation de l'infection

Le programme nuisible que l'on souhaite diffuser doit d'abord être développé. Cette phase n'est cependant pas nécessaire lors de chaque phase d'infection. Une fois le code nuisible développé par l'auteur de logiciels malveillants, ce dernier peut créer de nouvelles variantes à partir de ce modèle. Il dispose pour cela de « runtime packers », de compilateurs et outils de dissimulation du code, dans la mesure où le programme n'est pas déjà reconnu par les logiciels antivirus. Les pirates ne voulant pas développer eux-mêmes le code, peuvent en acheter dans

les forums clandestins. Une fois le programme nuisible disponible, le pirate choisit la ou les voies de diffusion. Le programme nuisible peut par exemple être exécuté par le biais d'une attaque automatique visant une faille de sécurité. Le pirate peut également utiliser une autre astuce pour pousser l'utilisateur à lancer le programme malveillant. Dans le premier cas, le pirate a besoin d'un code « exploit » qui prend le contrôle de l'ordinateur, dans le deuxième cas, d'un site Web, d'un courrier électronique ou d'un message instantané séduisant qui incite l'utilisateur à télécharger et exécuter le fichier. Si le programme nuisible est hébergé par un site Web, les domaines doivent être enregistrés et les fichiers correspondants doivent être intégrés au site. Il existe des outils facilitateurs, dédiés à la plupart de ces activités.

3.2 Exécution

Une fois l'ordinateur sous contrôle, un outil de téléchargement de type cheval de Troie est généralement lancé. Il veille à ce que les fichiers nuisibles soient chargés et lancés sur l'ordinateur. L'auteur de l'attaque est ensuite informé du succès de l'infection et de la prise de contrôle du système. Les paramètres de sécurité de l'ordinateur PC infecté sont ensuite restreints. Les autres activités du logiciel malveillant sont ainsi exécutées plus facilement. L'étape suivante consiste à charger d'autres logiciels malveillants sur l'ordinateur. Plusieurs fichiers nuisibles peuvent être nécessaires à l'exécution de cette étape. Dans de nombreux cas, le premier fichier nuisible chargé est une porte dérobée. L'ordinateur change alors de propriétaire : le pirate peut faire ce qu'il souhaite. La porte dérobée permet notamment de coordonner l'ordinateur, avec de nombreux autres ordinateurs PC du monde entier, via IRC, P2P ou HTTP. L'ordinateur fait alors partie d'une gigantesque armée de zombies. Une fois la porte dérobée installée, le système infecté est inspecté de manière scrupuleuse et le pirate décide de ce qu'il veut faire de l'ordinateur. Un logiciel espion recherche les données exploitables de l'ordinateur piraté. Des logiciels publicitaires peuvent également être installés. Si l'ordinateur dispose d'une connexion efficace à Internet, il peut être utilisé pour l'envoi de spam ou pour l'hébergement de fichiers illégaux, de sites Web d'hameçonnage ou de logiciels malveillants.

3.3 Utilisation de l'ordinateur infecté

Si l'ordinateur zombie d'un réseau est utilisé pour l'envoi de pollupostage, l'exploitant du réseau de zombies exécute, par le biais d'une porte dérobée, un logiciel malveillant, contenant notamment le modèle de courrier, une liste d'adresses électroniques et le logiciel d'envoi des courriers, sur l'ordinateur infecté. Une fois les fichiers installés, ils sont lancés et l'envoi commence. Une fois tous les courriers envoyés, le logiciel est supprimé avec l'ensemble des données de l'ordinateur. Seule la porte dérobée demeure, bien cachée, en attente de nouvelles instructions.

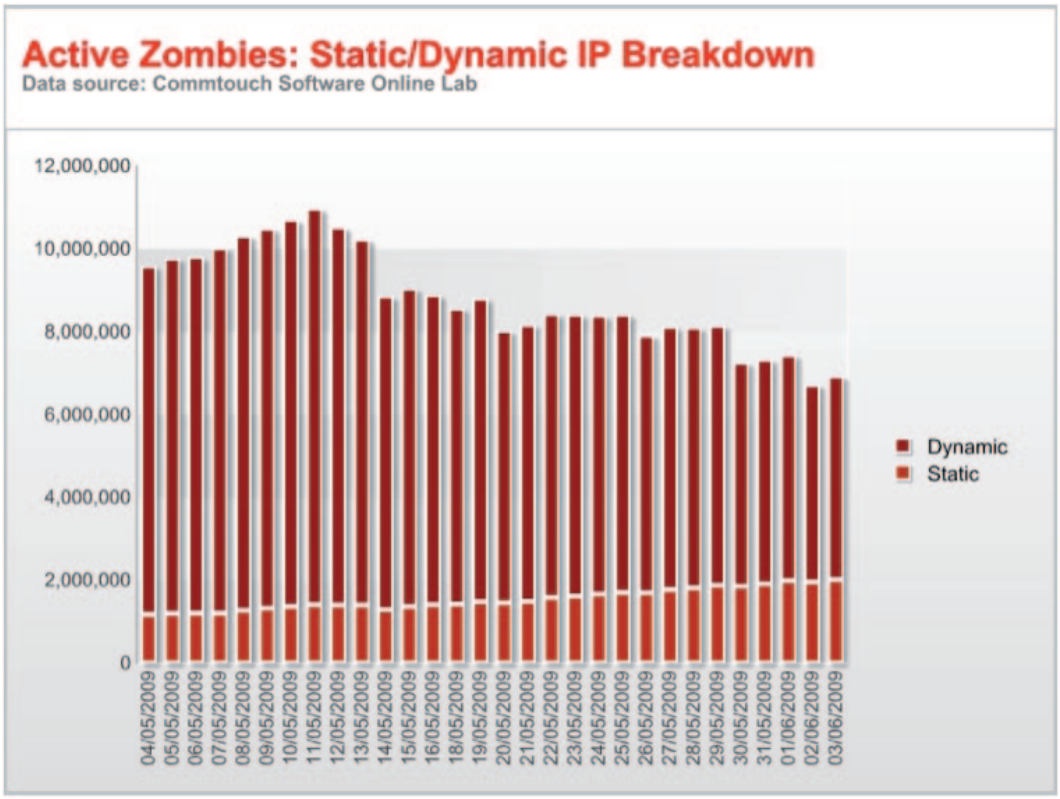
4. Conséquences des infections

Une fois le ou les PC infectés, les cyberdélinquants ont toutes les cartes en main pour gagner de l'argent. Présentation des quelques méthodes les plus utilisées.

4.1 Les réseaux zombies

Les réseaux de zombies sont le pivot de l'infrastructure de la criminalité électronique. Ils ne servent pas seulement à envoyer du spam ou à lancer des attaques par déni de service. Les ordinateurs zombies sont également utilisés pour héberger des pages de logiciels malveillants ou d'hameçonnage.

À l'origine, la gestion s'effectuait quasiment exclusivement par IRC (Internet Relay Chat, système de conversations textuelles en ligne). Lors des phases de développement suivantes, de plus en plus de réseaux de zombies utilisant d'autres protocoles pour la gestion sont apparus. Les réseaux de zombies les plus modernes, tels que le réseau Sturm, sont créés sur le système du réseau pair-à-pair (P2P) : aucun serveur n'est utilisé pour la communication des ordres, ce qui rend ce réseau difficilement détectable. Le tout aussi puissant réseau Zunker communique quant à lui via le protocole HTTP. Suite à la fermeture de McColo, un fournisseur de services Internet douteux, certains réseaux de zombies ont perdu leur ordinateur de commande et sont devenus ingérables. Les réseaux de zombies Srizbi et Storm ont notamment disparu. Les nouveaux réseaux de zombies, tels que Waledac ou Conficker, disposent désormais de nombreuses possibilités de contact.



Ill. 5 : Les PC zombies avec IP fixe augmentent. Les IP fixes sont le plus souvent utilisées par les entreprises.

4.2 Spam

Le spam est un marché considérable. Il ne rapporte pas seulement aux personnes qui proposent les produits. L'envoi de spams s'effectue généralement par le biais de réseaux de zombies. Si les ordinateurs d'une entreprise sont contaminés, des milliers (voire des millions) de courriers peuvent être envoyés chaque jour via cette connexion Internet. Ceci entraine plusieurs problèmes. La connexion Internet peut tout d'abord être ralentie par ces envois massifs. De nombreuses remontées de salariés concernant la lenteur de la connexion Internet doivent alerter les administrateurs du réseau. Autre problème : si trop d'envois non désirés sont envoyés via la ligne Internet de l'entreprise, l'adresse IP de la ligne peut être répertoriée dans les listes noires des logiciels de spam. Une situation embêtante puisque tous les courriers envoyés par les salariés seront alors répertoriés chez leurs correspondants comme étant du spam.

4.3 Chantage

Si la boutique en ligne d'une société est très lucrative ou si une entreprise dépend du traitement immédiat des courriers électroniques, il est possible d'exercer un chantage sur l'organisation en attaquant les services en question. Les ordinateurs zombies d'un réseau peuvent bombarder un site Web ou un serveur de messagerie de requêtes. Cette demande

massive surcharge le système au point que celui-ci ne peut plus fonctionner normalement. Pour retrouver un trafic normal, l'entreprise doit bien souvent payer. Ces attaques par saturation (en anglais, attaques de type Distributed Denial of Service ou

DDoS) peuvent toucher toutes les entreprises présentent sur Internet. Mais des attaques par saturation sont également utilisées à des fins politiques. Entre la fin avril et le

début mai 2007, les serveurs de ministères, agences gouvernementales, banques, journaux et d'entreprises d'Estonie ont été paralysés. Dans ce cas, les réseaux de zombies ont été clairement utilisés comme outil politique.

Hormis le chantage via DDoS, il existe d'autres possibilités d'extorquer de l'argent aux victimes. Les logiciels de rançon, tels que GPCoder, chiffrent certains fichiers d'un ordinateur. Si vous souhaitez de nouveau accéder au contenu des fichiers, vous devez acheter un programme de déchiffrement, vendu entre 12 et 200 dollars.

Il existe un autre modèle dans les entreprises. Un cheval de Troie peut transférer des images de pornographie infantile, des logiciels illégaux et/ou des fichiers audio et vidéo protégés contre la copie sur l'ordinateur infecté d'un collaborateur. Le pirate peut alors menacer le collaborateur d'informer son responsable ou menacer l'entreprise de présenter les documents à la police.

4.4 Vol de données

L'entreprise regorge de documents confidentiels et de données privées. Chez un particulier, les données bancaires ou de carte de crédit sont les principales cibles. Dans les entreprises, toute donnée peut être revendue. Lancement stratégique et marketing, technologies en développement, brevet sont autant d'informations qui peuvent intéresser les concurrents. Et ce ne sont pas les seules informations intéressantes. Les bases de données de clients ou d'employés sont d'autres fichiers très prisés. Ces données, revendues sur le marché parallèle peuvent être utilisées dans le cadre d'attaque d'hameçonnage ou de spam.

L'intrusion sur les réseaux mise à part, le vol de donnes peut aussi se réaliser à l'aide d'enregistreurs de frappes. Il s'agit de programmes qui enregistrent les éléments saisis au clavier. Ces outils permettent de voler en temps réel tout type d'information. Les codes d'accès à des serveurs d'entreprise, le contenu de documents et de courriers électroniques confidentiels ou encore les données d'accès à des serveurs, des forums et des réseaux privés virtuels sont autant d'actions possibles. Si un serveur Web réparé est de nouveau infecté au bout de quelques jours, étudiez la possibilité du vol des mots de passe administrateur par un enregistreur de frappes. Des fichiers de registre de tels enregistreurs de frappes sont proposés sur les forums clandestins à des prix de quelques centaines d'euros pour des dizaines de Gigaoctets.

5. Les moyens de protection

La protection des ordinateurs d'entreprise contre les logiciels malveillants est un domaine de

la sécurité informatique qui doit être mise en relation avec l'ensemble de la sécurité informatique d'une entreprise. La sécurité informatique n'est pas un état, mais un processus.

Chaque entreprise compte des services ou groupes d'utilisateurs particulièrement menacés

et ayant besoin d'une protection spécifique. Dans le cadre de ce processus, chaque entreprise doit prendre une multitude de décisions aboutissant à des solutions totalement personnalisées. Pour commencer, on associe la protection contre les logiciels malveillants à la mise en application de procédures techniques qui doivent protéger ou protègent de menaces définies. Les principales mesures techniques sont les suivantes :

- **Protection antivirus**
  Elle doit être installée aussi bien sur les serveurs que sur les clients. Elle doit également s'assurer de l'absence de codes nuisibles au niveau des flux de données HTTP et, le cas échéant, des données de chats (ICQ, IRC).
- **Protection contre le spam**
  Les courriers électroniques contenant désormais des liens vers les sites Web nuisibles à la place de fichiers en pièce jointe, la protection contre le spam doit être exécutée en parallèle avec la protection contre les logiciels malveillants.
- **Pare-feu, détection/prévention contre les intrusions**
  Les données du trafic réseau peuvent être utilisées pour détecter et empêcher les attaques des vers Internet courants. D'autres mesures techniques contribuent également à la protection antivirus. La gestion des correctifs, la virtualisation des logiciels, les droits d'utilisation des ordinateurs d'entreprise, le contrôle des accès aux fichiers et zones réseau, ainsi que de nombreuses autres mesures préventives complètent les mesures de sécurité notoires.

Les mesures techniques ne suffisent malheureusement pas à protéger efficacement un réseau d'entreprise. Les mesures de sécurité doivent être acceptées et soutenues par les employés. L'utilisation des ordinateurs, des supports de données et autres informations pertinentes à la sécurité doit être définie par la direction. Un cadre indispensable à la sensibilisation des salariés. Des dispositions juridiques et éthiques sont aussi à prendre en compte. Pour terminer, les employés doivent être informés des sources de dangers sur

Internet et dans leur travail de tous les jours. Le respect des mesures techniques des employés attentifs préserve les ordinateurs de l'entreprise des logiciels malveillants.