

SÉCURITÉ INFORMATIQUE

**Règles pratiques et solutions
à appliquer en entreprise**

> LA SÉCURITÉ DU COURRIEL <

TABLE DES MATIÈRES

LE CONTEXTE DE LA SÉCURITÉ DU COURRIEL	3
L'INDUSTRIE DU SPAM	4
LE « HARVESTING » OU RÉCOLTE DES ADRESSES	4
ZOMBIES ET BOTNETS OU LES ARMÉES SILENCIEUSES	5
UN UNIVERS DE MENACES.....	6
NATURE DES RISQUES ASSOCIÉS AU COURRIEL	6
Le SPAM	6
Les virus	7
L'hammeçonnage.....	8
Les fichiers exécutables.....	9
Le bruit.....	9
LE COURRIEL – UN CANAL INSÉCURÉ PAR DÉFINITION.....	10
LES COÛTS ASSOCIÉS AUX MENACES.....	11
Les coûts directs	11
Perte de productivité	11
Bande passante (aggravation de la menace).....	12
Impact sur les ressources	12
Les coûts indirects.....	12
Perte de confiance	13
Détresse psychologique.....	13
Accroissement des coûts pour les envoyeurs massifs	13
Enveloppe ou contenu?.....	15
Techniques de blocage d'enveloppe.....	16
Listes noires.....	16
Les Rbls (Real time blackhole lists) ou DNSbl (DNS blackhole lists).....	16
SPF et DKIM	17
Intégrité SMTP	18
LE FILTRAGE DE CONTENU.....	19
Un mot sur le camouflage du contenu (<i>obfuscation techniques</i>).....	20
Les mots clés	20
Les expressions régulières	20
Les heuristiques – Spam Assassin.....	20
Le filtrage statistique – Bayes / CRM114 / DSPAM.....	22
Filtrage d'URL	22
Les signatures – RAZOR / PHYZOR / DCC	22
Les « SVM Support Vector machine »	23
Le « greylisting »	19
a) Les solutions client.....	23
b) Les solutions passerelles.....	24
Sécurité	24
Mises à jour.....	24
Coûts en capital	25
Un seul MX protégé	25
Consommation des ressources	25
c) Les solutions en amont	26
LA LOI.....	28
Contexte américain	28
Contexte européen	28
Contexte canadien	29
CONCLUSION.....	29

LE CONTEXTE DE LA SÉCURITÉ DU COURRIEL

De nos jours, toutes les entreprises doivent évoluer dans un monde de plus en plus ouvert, de plus en plus connecté. Depuis les années 2000, l'accès global à Internet dans l'environnement corporatif est devenu monnaie courante. Bien peu de sociétés ou d'organismes publics peuvent aujourd'hui mener leurs affaires sans que leurs employés disposent d'une adresse de courrier électronique.

D'ailleurs, dans un nombre grandissant d'industries, le courriel a désormais plus de valeur que le téléphone comme moyen de communication privilégié, car il permet un accès asynchrone non intrusif et peut véhiculer divers contenus; images, documents et vidéos. Plusieurs études ont démontré que près de 60 % de l'information critique à la conduite des affaires se retrouve dans les boîtes de courriel des employés.

Les gestionnaires TI considèrent que le courrier électronique est une application primordiale, dont il faut se préoccuper en tout temps et qui doit jouir d'une disponibilité complète, 24 heures par jour, 365 jours par année.

Ainsi, les réseaux d'entreprises sont maintenant presque tous connectés d'une façon ou d'une autre au réseau Internet. Or, parallèlement à la progression de l'Internet, tout un univers de menaces visant les entreprises et le secteur résidentiel s'est aussi développé.

La première manifestation du risque de la connectivité globale s'est produite en mai 2000 avec le virus « I love you » qui a infecté 45 millions de machines en utilisant la capacité du logiciel client Microsoft Outlook d'exécuter des scripts vbs. Cette infection a attiré l'attention des médias et sensibilisé les gestionnaires à la vulnérabilité de l'application qui allait devenir le vecteur principal de transport des menaces dans leurs entreprises : le courrier électronique. On estime que le virus a causé plus de 10 milliards \$US en pertes et dommages de toutes natures.

Ce virus était aussi un exemple de l'une des premières utilisations de ce qu'il est convenu d'appeler les techniques d'ingénierie sociale, c'est-à-dire l'utilisation d'une argumentation convaincante pour inciter le destinataire à poser un geste précis qui compromet sa sécurité. En effet, qui aurait pu se méfier d'une missive au titre si engageant et en apparence inoffensif?

Aujourd'hui, les techniques d'ingénierie sociale sont couramment utilisées lors d'attaques de phishing (hameçonnage) pour convaincre les clients d'institutions financières de cliquer sur des liens qui les dirigent vers des sites factices, en vue d'intercepter leurs informations d'accès et leurs données personnelles.

L'épisode « I love you » a eu pour effet de convaincre ceux qui étaient encore sceptiques de la nécessité d'acquiescer et de tenir à jour un antivirus de première qualité. La protection antivirale est maintenant considérée, à juste titre, comme une dépense normale, absolument nécessaire pour l'exploitation saine d'un ordinateur.

« I love you » a aussi démontré comment les failles de sécurité dans les logiciels grand public pouvaient être exploitées à des fins malveillantes. C'est d'ailleurs à partir de ce moment que la fréquentation de plusieurs sites comme le *CERT*, le *CIAC*, *SecurityFocus* le *SANS institute*, tous consacrés à la sécurité, a connu une véritable explosion.

L'INDUSTRIE DU SPAM

À la fin des années 90, avec la possibilité de gains faciles comme élément propulseur, le pourriel a donné naissance à toute une économie souterraine. Grâce à la nouveauté du phénomène du pourriel et à cause des multiples vulnérabilités des systèmes de l'époque, les premiers polluposteurs sont ceux qui ont eu le plus de succès. Avec peu de barrières à l'entrée et un vaste choix de vecteurs, ils étaient en position d'obtenir un taux de clics de l'ordre de 1 à 2 %, ce qui est excellent par comparaison aux taux actuels qui sont de l'ordre de 1 sur 100 000 et moins.

Ne pas confondre le messager et le vendeur

Le polluposteur n'est pas le vendeur du produit. Il est là pour relayer un message promotionnel au plus large auditoire possible. En ce sens, il désire camoufler son identité et amener le client à poser un geste comme visiter un site Web, installer un logiciel ou composer un numéro de téléphone. Le polluposteur peut agir comme agent du vendeur, mais il ne vend jamais lui-même. Il est rémunéré à partir des ventes issues de sa campagne de diffusion. Généralement, le polluposteur dispose d'un identificateur unique dans le lien proposé et c'est cet identificateur qui permet au vendeur de comptabiliser les transactions générées par chaque agent.

Le lien entre l'envoyeur et l'acheteur peut être indirect et peut passer par une longue chaîne d'intermédiaires, de sorte qu'il devient quasi impossible de remonter jusqu'à la source. Les « lead generators » ou « trafic generators » vendent leurs services aux entreprises qui cherchent à générer du trafic sur leur site de commerce électronique. Les « lead generators » peuvent sous-contracter avec des intervenants, qui achètent ce type de service d'autres intervenants, plus ou moins scrupuleux, et ainsi de suite. Les entreprises qui utilisent les services de ces intermédiaires se défendent bien de faire du pollupostage mais elles sont les premières à en bénéficier. Certaines d'entre elles vont même pousser l'hypocrisie jusqu'à interdire à leurs agents de faire du pollupostage alors qu'en pratique, elles le tolèrent jusqu'au moment où elles font face à une plainte ou à une enquête. Situation qu'elles utilisent alors à leur avantage pour se débarrasser de l'agent en cause, tout en prenant soin, au passage, d'annuler toutes les commissions, ristournes ou redevances qui lui seraient dues.

Il y a maintenant une industrie florissante qui offre aux polluposteurs une gamme complète de services et de logiciels spécialisés. En plus du classique logiciel d'envoi massif, on trouve aujourd'hui des bases de données d'adresses, des services impartis d'envois, des validateurs d'adresses automatisés, des robots extracteurs, des réseaux infectés (BOT Nets) à vendre ou à louer, ainsi que des hébergeurs et des registraires complaisants.

LE « HARVESTING » OU LA RÉCOLTE DES ADRESSES

Le « *harvesting* » est le processus automatisé à partir duquel une adresse électronique est découverte et intégrée à une liste d'envoi. Si une adresse électronique est publiée sur un site Web, elle aura toutes les chances de se retrouver intégrée à des campagnes d'hameçonnage en premier lieu, et ensuite, d'être ajoutée à des listes de pollupostage.

Les polluposteurs utilisent des robots fort similaires à celui utilisé par Google® pour extraire chaque adresse de courriel pouvant apparaître sur une page Web. Ces robots ont des noms aussi exotiques que :

- *autoemailspider*
- *Wordpress Hash Grabber*
- *Missigua Locator 1.9*
- *Digger*
- *EmailSiphon*

Les « *harvesters* » constituent donc pour ainsi dire le point de départ de la chaîne de propagation du pourriel. Ils utilisent le plus souvent des serveurs avec des adresses IP statiques sur des liens à haute capacité. Cette façon de procéder les rend plus vulnérables car elle facilite leur identification. Toutefois, le risque lié aux opérations de « *harvesting* » n'est pas très grand car il existe un vide juridique autour de cette activité qui n'est pas expressément interdite par la loi.

Le projet « *honeypot* » voir www.projecthoneypot.org a permis de faire le lien entre le « *harvesting* » et l'utilisation d'une adresse de courriel, dévoilant ainsi des informations précieuses sur la manière dont les réseaux de cueillette d'adresses de courriel opèrent. Le principe du piège est simple, mais ingénieux; chaque participant cède un pointeur MX sur un sous-domaine ou un domaine non utilisé. Le pointeur MX est dirigé vers un des multiples serveurs liés au projet. Le participant place sur une page Web un lien vers une page piégée qui générera une adresse électronique unique sur le domaine cédé. Ensuite, dès qu'un courriel est reçu à cette adresse fictive, le lien peut être fait entre le robot et l'envoi du message.

ZOMBIES ET BOTNETS OU LES ARMÉES SILENCIEUSES

Les cyber-criminels ont tôt fait de comprendre qu'ils pouvaient utiliser les failles de sécurité des systèmes d'exploitation, des fureteurs et des diverses composantes logicielles pour infecter d'innocentes victimes et transformer leur ordinateur en plateforme d'envoi et d'attaque. Ces ordinateurs infectés, aussi appelés zombies, sont reliés en réseaux qu'on appelle des « *botnets* ». Les « *botnets* » peuvent comprendre de 10 000 à un million de participants. Chaque « *botnets* » obéit à un centre de commande et de contrôle absolument invisible qui décide des attaques à mener.

Aujourd'hui, on considère que 60 à 80 % du pourriel provient de « *botnets* ». Les « *botnets* » sont aussi en excellente position pour mener des attaques de déni de service (*Denial of service attacks* ou *DDOS*), des balayages de vulnérabilité réseau, des attaques d'intrusion de force brute et d'autres formes d'agressions réseau. L'année 2005 a connu une formidable explosion du nombre de « *botnets* » et de leur niveau de sophistication.

UN UNIVERS DE MENACES

L'univers des menaces auxquelles sont exposées les organisations en matière de sécurité des systèmes est extrêmement vaste et il évolue constamment. Loin de se limiter aux risques associés au courrier électronique, cet univers comprend une foule d'autres risques :

- Les risques liés aux systèmes d'exploitation et aux composantes logicielles
- Les risques liés aux logiciels d'application
- Les risques liés aux appareils dédiés come les coupe-feu et les routeurs
- Les applications développées à l'interne
- Les intrusions réseau
- Les réseaux sans fils
- Les logiciels espions
- Les interceptions des données et du trafic réseau
- Les accès non autorisés
- La perte ou la divulgation d'informations confidentielles.

Tout responsable de la sécurité devrait évaluer son niveau de risque et adopter les mesures de protection qui s'imposent en fonction de la valeur des actifs à protéger et de la probabilité que la menace se réalise.

Ceci dit, tous conviennent que la première source de vulnérabilité, celle qui se manifeste de manière constante, 24 heures par jour, est celle liée au courrier électronique.

NATURE DES RISQUES ASSOCIÉS AU COURRIEL

Le SPAM

Le spam représente la menace principale associée au courrier électronique. Le volume de spam en circulation a atteint environ 85 % des connexions SMTP. Cela signifie que, sur un serveur moyen, plus de huit connexions sur dix sont nuisibles. C'est comme si le raccordement au réseau d'aqueduc de votre résidence perdait 75 % de l'eau qui y circule. Il arrive aussi que des domaines fassent l'objet d'attaques de dictionnaire où un expéditeur malveillant, habituellement en provenance d'un botnet, tente d'identifier les adresses valides en itérant séquentiellement des connexions sur des combinaisons de caractères qui composent l'adresse. Même pour des domaines relativement modestes, qui utilisent de 50 à 100 boîtes de courriel, le nombre de connexions quotidiennes générées par ces attaques peut atteindre plusieurs dizaines de milliers et congestionner complètement le réseau et le serveur de destination de la victime.

```

Dec 30 12:53:30 filter postfix/smtpd[18131]: NOQUEUE: reject: RCPT from unknown[218.71.255.225]: 554 <aamda@flexis.com>;
Recipient address rejected: INVALID ADDRESS; from=<tarraion@iloveyoulord.com> to=<aamda@flexis.com> proto=SMTP helo=<iloveyoulord.com>
Dec 30 12:53:30 filter postfix/smtpd[18258]: NOQUEUE: reject: RCPT from unknown[218.71.255.225]: 554 <a.alina@flexis.com>;
Recipient address rejected: INVALID ADDRESS; from=<claudiah@guideshop.com> to=<a.alina@flexis.com> proto=SMTP helo=<guideshop.com>
Dec 30 12:53:30 filter postfix/smtpd[18131]: NOQUEUE: reject: RCPT from unknown[218.71.255.225]: 554 <a8602520@flexis.com>;
Recipient address rejected: INVALID ADDRESS; from=<tarraion@iloveyoulord.com> to=<a8602520@flexis.com> proto=SMTP helo=<iloveyoulord.com>
Dec 30 12:53:31 filter postfix/smtpd[17037]: connect from unknown[222.76.147.206]
Dec 30 12:53:31 filter postfix/smtpd[17059]: connect from host2-137.pool8258.interbusiness.it[82.58.137.2]
Dec 30 12:53:31 filter postfix/smtpd[17952]: NOQUEUE: reject: RCPT from unknown[218.71.255.225]: 554 <aa8bj@flexis.com>;
Recipient address rejected: INVALID ADDRESS; from=<trystan@k9gear.net> to=<aa8bj@flexis.com> proto=SMTP helo=<k9gear.net>
Dec 30 12:53:32 filter postfix/smtpd[17951]: NOQUEUE: reject: RCPT from 22.Red-80-59-171.staticIP.rima-tde.net[80.59.171.22]: 554 <a.valerie@flexis.com>;
Recipient address rejected: INVALID ADDRESS; from=<dyzeori@optonline.com> to=<a.valerie@flexis.com> proto=SMTP helo=<lh>
Dec 30 12:53:32 filter postfix/smtpd[17037]: NOQUEUE: reject: RCPT from unknown[222.76.147.206]: 554 <aallx@flexis.com>;
Recipient address rejected: INVALID ADDRESS; from=<Anglicanizes@noahonline.net> to=<aallx@flexis.com> proto=SMTP helo=<222.76.147.206>
Dec 30 12:53:32 filter postfix/smtpd[17059]: NOQUEUE: reject: RCPT from host2-137.pool8258.interbusiness.it[82.58.137.2]: 554 <a.corey@flexis.com>;
Recipient address rejected: INVALID ADDRESS; from=<BriceBoldenapocalypse@gordonmumford.com> to=<a.corey@flexis.com> proto=SMTP helo=<host2-137.pool8258.interbusiness.it>
Dec 30 12:53:32 filter postfix/smtpd[17037]: disconnect from unknown[222.76.147.206]
Dec 30 12:53:33 filter postfix/smtpd[17059]: NOQUEUE: reject: RCPT from host2-137.pool8258.interbusiness.it[82.58.137.2]: 554 <a.pandhi@flexis.com>; Recipient address
rejected: INVALID ADDRESS; from=<BriceBoldenapocalypse@gordonmumford.com> to=<a.pandhi@flexis.com> proto=SMTP helo=<host2-137.pool8258.interbusiness.it>
...
Dec 30 12:53:40 filter postfix/smtpd[17953]: connect from m57.net85-169-179.noos.fr[85.169.179.57]
Dec 30 12:53:41 filter postfix/smtpd[17037]: NOQUEUE: reject: RCPT from clj167.neoplus.adsl.tpnet.pl[83.31.111.167]: 554 <aaron6006@flexis.com>;
Recipient address rejected: INVALID ADDRESS; from=<bilinear@cvrbo.com> to=<aaron6006@flexis.com> proto=SMTP helo=<clj167.neoplus.adsl.tpnet.pl>
Dec 30 12:53:41 filter postfix/smtpd[18257]: NOQUEUE: reject: RCPT from ds15400CD41.pool1.t-online.hu[84.0.205.65]: 554 <a711203@flexis.com>;
Recipient address rejected: INVALID ADDRESS; from=<qjali@optonline.com> to=<a711203@flexis.com> proto=SMTP helo=<lh>
Dec 30 12:53:41 filter postfix/smtpd[17037]: disconnect from clj167.neoplus.adsl.tpnet.pl[83.31.111.167]
Dec 30 12:53:42 filter postfix/smtpd[17951]: NOQUEUE: reject: RCPT from 22.Red-80-59-171.staticIP.rima-tde.net[80.59.171.22]:
554 <aaqlu@flexis.com>;
Recipient address rejected: INVALID ADDRESS; from=<Dyzeori@optonline.com> to=<aaqlu@flexis.com> proto=SMTP helo=<lh>
Dec 30 12:53:43 filter postfix/smtpd[18134]: connect from ip-85-160-31-182.eurotel.cz[85.160.31.182]
Dec 30 12:53:43 filter postfix/smtpd[17059]: NOQUEUE: reject: RCPT from host2-137.pool8258.interbusiness.it[82.58.137.2]: 554 <a.p.bobbink@flexis.com>; Recipient address
rejected: INVALID ADDRESS; from=<BriceBoldenapocalypse@gordonmumford.com> to=<a.p.bobbink@flexis.com> proto=SMTP helo=<host2-137.pool8258.interbusiness.it>
Dec 30 12:53:45 filter postfix/smtpd[18134]: NOQUEUE: reject: RCPT from ip-85-160-31-182.eurotel.cz[85.160.31.182]: 554 <aaooaa1@flexis.com>;
Recipient address rejected: INVALID ADDRESS; from=<ashes@allsportbook.com> to=<aaooaa1@flexis.com> proto=SMTP helo=<ip-85-160-31-182.eurotel.cz>
Dec 30 12:53:45 filter postfix/smtpd[18134]: disconnect from ip-85-160-31-182.eurotel.cz[85.160.31.182]
Dec 30 12:53:47 filter postfix/smtpd[17043]: NOQUEUE: reject: RCPT from unknown[203.101.162.170]: 554 <aan47yowk4@flexis.com>;
Recipient address rejected: INVALID ADDRESS; from=<bombardment@fbc.lamar.org> to=<aan47yowk4@flexis.com> proto=SMTP helo=<tramontana.eutelsat.net>
Dec 30 12:53:48 filter postfix/smtpd[17039]: NOQUEUE: reject: RCPT from unknown[59.35.165.103]: 554 <a-bradbe@flexis.com>;
Recipient address rejected: INVALID ADDRESS; from=<mfayce@optonline.com> to=<a-bradbe@flexis.com> proto=SMTP helo=<lh>
Dec 30 12:53:49 filter postfix/smtpd[17953]: NOQUEUE: reject: RCPT from m57.net85-169-179.noos.fr[85.169.179.57]: 554 <aaron164@flexis.com>;
Recipient address rejected: INVALID ADDRESS; from=<JeanineMartiniroquois@lucutus.com> to=<aaron164@flexis.com> proto=SMTP helo=<m57.net85-169-179.noos.fr>

```

30 connexions nocives en 19 secondes
 -> 90 connexions / minutes
 -> 129600 connexions / jour

Exemple de surcharge liée à une attaque de dictionnaire (menace aggravée)

Le spam est donc une menace à fréquence élevée mais son un niveau de dangerosité est relativement bas. Plus récemment on a vu des campagnes de pourriel diriger le trafic vers des sites dangereux qui infectaient le poste du visiteur et tentaient de l'intégrer à un réseau de BOT Nets. Le niveau de dangerosité s'est ainsi instantanément accru.

Les virus

Le courriel est devenu le vecteur principal de propagation des virus. Nos statistiques démontrent qu'environ un courriel sur 1000 transporte un virus. Ceux-ci sont nombreux et en constante évolution et la prévalence varie dans le temps. Il existe maintenant des troussees de création de virus et des engins de polymorphisme qui permettent aux virus de se modifier à chaque transmission. Ils sont écrits par des experts qui sont eux-mêmes de plus en plus qualifiés et de mieux en mieux outillés pour accomplir leur œuvre. Si, par le passé, certains virus n'avaient d'autre objectif que de glorifier leur créateur, il en va tout autrement aujourd'hui car les virus sont les agents recruteurs des futurs zombies, ces soldats obéissants qui forment une armée silencieuse et dont la création sera rentabilisée

par l'envoi de spam, par l'exécution de campagnes d'hameçonnage ou par la perpétration d'attaques réseau systématiques.

Avec le temps, les créateurs de virus ont réussi à réduire sensiblement le délai de mise en œuvre de leur arme, c'est-à-dire le temps qui s'écoule entre le moment où une rustine devient disponible pour une vulnérabilité identifiée et le moment où un virus est propagé pour exploiter cette vulnérabilité chez les utilisateurs qui ont négligé de se procurer la rustine en question. Ainsi, le virus « Nimda », qui exploitait une faille dans Windows (www.microsoft.com/technet/security/bulletin/MS00-078.msp), est né 336 jours (soit près d'un an) après l'émission de la rustine de Microsoft. Le virus « Sasser », pour sa part, a été découvert seulement 17 jours après la parution de la rustine Microsoft (www.microsoft.com/technet/security/bulletin/MS04-011.msp). Voilà qui prouve que les auteurs de virus sont maintenant capables de réagir très rapidement et qu'ils exploiteront systématiquement les systèmes qui ne sont pas rigoureusement tenus à jour.

La menace virale par courriel est une menace à basse fréquence mais elle présente un niveau de dangerosité élevé. Cette dangerosité se trouve multipliée dans le contexte des grandes organisations où une seule personne imprudente, un seul poste mal protégé suffisent pour déclencher une infection majeure.

L'hameçonnage

Le « phishing », ou hameçonnage, est une menace plus récente, qui est apparue pour la première fois en 2003. L'hameçonnage se définit comme suit :

L'utilisation d'un courriel prétendant provenir d'une source légitime, dans le but d'obtenir des consommateurs qu'ils divulguent à leur insu des renseignements personnels.

L'hameçonnage vise généralement les clients des institutions financières ou des sociétés offrant des services de traitement de paiement. Il ne faut donc pas s'étonner que Paypal® et eBay® figurent en bonne position dans le palmarès des sociétés dont les marques sont usurpées. Les victimes sont les clients crédules de ces institutions qui se sont rendus sur les sites factices et ont dévoilé leurs informations personnelles; numéros de carte bancaire, numéros de comptes, numéros d'identification personnels et codes d'accès. Les travailleurs peuvent compter parmi ces victimes et leur adresse électronique au bureau peut être utilisée pour les berner. Généralement, en cas de fraude, les institutions financières vont protéger et indemniser leurs clients victimes de tentatives d'hameçonnage. Pour les victimes, l'histoire ne s'arrête pas là car elles devront travailler à rétablir leur dossier de crédit si celui-ci a été entaché par des transactions frauduleuses réalisées à l'aide de leurs informations personnelles.

Au Canada, presque toutes les institutions financières ont fait l'objet de tentatives d'hameçonnage. On assiste aujourd'hui à des campagnes plus ciblées, ce qui confirme que les hameçonneurs raffinent leurs procédés. En septembre 2005, une campagne qui visait la Banque Royale du Canada a rejoint plus de 22 000 adresses de courriel canadiennes dotées d'un suffixe « .ca ». Une autre campagne qui visait Desjardins a été envoyée en français. Il s'agissait d'un français de mauvaise qualité, certes, mais ce souci de s'adresser aux victimes dans leur langue témoigne de l'évolution de l'approche des auteurs des campagnes d'hameçonnage. La résilience et l'ingéniosité des campagnes d'hameçonnage ne cesse

d'augmenter. Les techniques d'ingénierie sociale se développent et se diversifient et n'hésitent pas à exploiter honteusement les causes les plus nobles. On a vu par exemple des cas d'hameçonnage immédiatement après le tsunami de décembre 2004 et l'ouragan Katrina. La lutte à l'hameçonnage s'organise mais elle pose des défis considérables, notamment à cause des registraires peu scrupuleux et des hébergeurs complaisants. La concurrence féroce entre les registraires et la guerre des prix à laquelle ils se livrent a provoqué l'apparition de registraires de second ordre offrant des services d'enregistrement à rabais mais sans offrir de services de sécurité et d'enquête en cas d'abus.

Les attaques se font souvent à l'aide de domaines enregistrés massivement et qui semblent avoir un lien avec la société victime ou avec l'une de ses marques de commerce, par exemple : *paypal-online.com*, *accesd.com*. Les domaines enregistrés à des fins frauduleuses peuvent être nombreux. On a déjà vu 80 domaines enregistrés et activés à l'intérieur d'une période de 24 heures pour coordonner une attaque d'hameçonnage contre une institution.

Les fichiers exécutables

Même s'ils ne contiennent pas de virus, les fichiers exécutables transmis par courriel peuvent néanmoins s'avérer inappropriés dans une organisation qui souhaite contrôler la configuration de ses postes de travail. Il peut s'agir de logiciels non approuvés, non testés ou dépourvus des licences requises et qui ne se conforment pas aux normes en vigueur. Pour toutes ces raisons, les organisations choisissent généralement de bannir tout fichier exécutable transmis par courriel directement à la passerelle de réception. On évite ainsi qu'un usager soit tenté d'ouvrir et d'exécuter de tels contenus.

Le bruit

Le niveau de bruit véhiculé par le courriel tant interne qu'externe est en augmentation. Le bruit représente toute communication inutile sans réelle valeur pour l'organisation. Dans cette catégorie, on retrouve les blagues de toutes sortes, les chaînes de lettres, les canulars, les fausses alarmes, les fichiers audio, les images et le contenu multimédia inapproprié. Une séquence vidéo .avi de 8 Mo envoyée à un grand nombre de destinataires peut causer des problèmes de congestion réseau et de surcharge des serveurs.

Le bruit constitue davantage une nuisance qu'une réelle menace. Les organisations qui, dans le cadre de leur politique de sécurité de l'information, adoptent des directives sur l'utilisation du courriel et investissent en formation, réussissent à mitiger l'impact du bruit sur leur réseau.

Le déni de service et les bombes de contenu

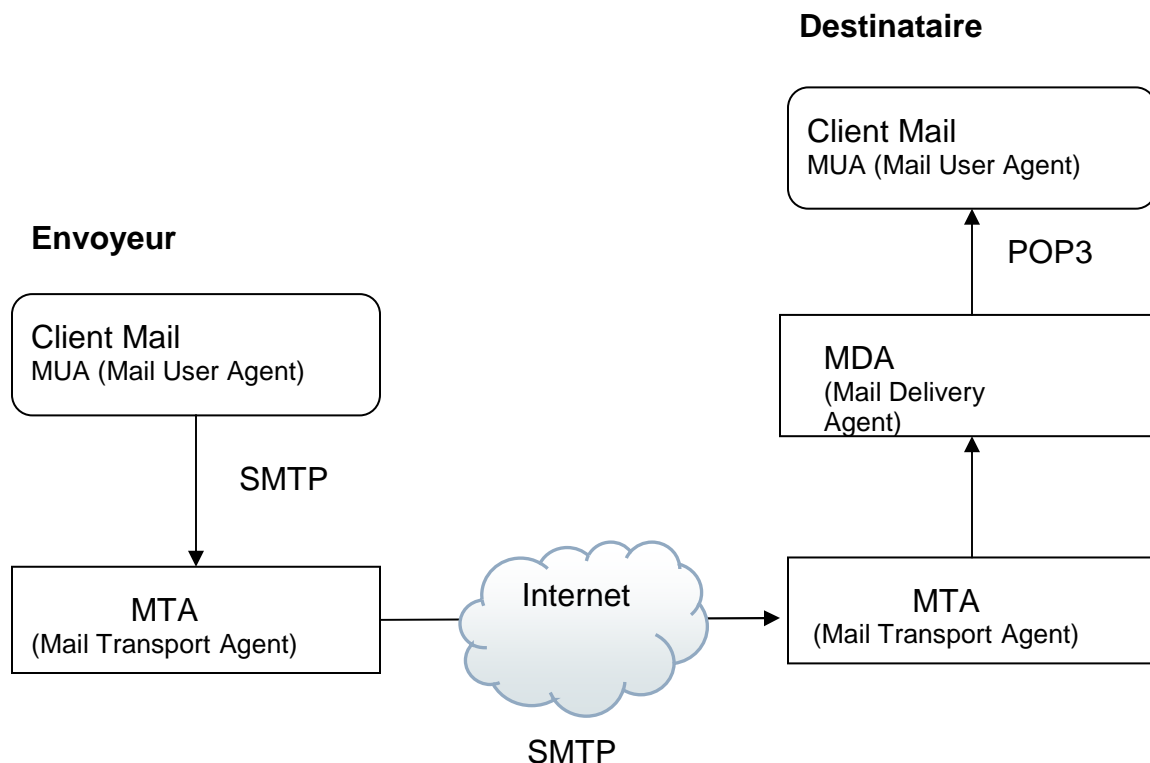
Lorsqu'un serveur ou un lien Internet deviennent saturés en raison d'une attaque externe, on parle de déni de service ou DOS – *Denial of service attack*. La plus connue de ces attaques est sans doute celle de MafiaBoy qui, au début de l'année 2000, a inondé de requêtes les sites Web de Yahoo®, Amazon® et eBay®.

Au niveau du courriel, des attaques similaires peuvent être lancées simplement en inondant une passerelle de messages. Selon le trafic généré, le serveur peut être en mesure de répondre à la demande ou non. Le déni de service est confirmé lorsque l'infrastructure n'est plus en mesure de fournir les services pour lesquels elle a été prévue. Lorsque le nombre de connexions dépasse le niveau de bruit normalement observé, on parle alors de menace aggravée. La perte se situe essentiellement au niveau de la bande passante.

Dans la même catégorie, les bombes de contenu peuvent avoir un effet similaire mais elles y parviennent d'une autre façon. La majorité des passerelles de courrier disposent des fonctions requises pour décompresser les messages en format *.zip* de façon à pouvoir en vérifier l'innocuité. Le stratagème consiste à envoyer des fichiers qui sont petits mais qui, une fois décompressés, exploseront littéralement en multipliant leur taille par un facteur astronomique. Un simple message de 6 Ko peut alors se transformer en un fichier de 100 Go tant et si bien que sa multiplication arrive à saturer la mémoire interne et l'espace disque et parvient à faire avorter un processus critique.

LE COURRIEL – UN CANAL INSÉCURÉ PAR DÉFINITION

Une autre dimension du risque associé au courriel se présente sous la forme de la perte possible de confidentialité. Prenons le cas d'une transmission courriel standard entre un expéditeur et un destinataire. L'expéditeur transmettra son message en mode plein texte en utilisant le protocole SMTP à sa passerelle d'entreprise. La passerelle relaiera le message au serveur de destination, toujours en mode plein texte, en utilisant le protocole SMTP. Finalement, après son arrivée au serveur de destination, le message sera transmis, toujours en mode plein texte, au client POP3 qui en fera la demande.



Ainsi, au cours de toutes les phases de sa transmission, le message a transité sur le réseau en mode plein texte. Il est donc facile pour un administrateur système ou pour quiconque est en mesure d'installer un dispositif de surveillance (ou « *packet sniffer* ») d'intercepter cette communication par courriel et de reconstruire le message transmis. À l'ère des réseaux sans fils non sécurisés, qui sont de plus en plus disponibles dans les cafés, gares, aéroports et autres lieux publics, il est primordial de tenir compte de cette vulnérabilité intrinsèque. Même si peu de cas ont fait les manchettes à ce jour, ce n'est qu'une question de temps avant que la quantité grandissante d'informations confidentielles non protégées qui circule par courriel sur les réseaux sans fils ne soit exploitée par des opportunistes sans scrupules.

Bien sûr, on peut avoir recours à des technologies de chiffrement pour protéger la confidentialité des communications. Ces technologies sont d'ailleurs de plus en plus utilisées et les cyber-criminels l'ont compris il y a longtemps. La plupart des entreprises font cependant le choix d'assumer le risque inhérent à la non confidentialité des communications et continuent d'utiliser le courriel en mode plein texte plutôt que de déployer des infrastructures de chiffrement.

LES COÛTS ASSOCIÉS AUX MENACES

Les coûts directs

S'il n'est pas endigué, le spam occasionnera des coûts directs de natures diverses pour l'organisation. Le risque d'occurrence élevé de ces pertes en tout genre justifie en fait largement le déploiement de mesures de protection.

Perte de productivité

La perte de productivité est de loin le principal argument en faveur de l'établissement de mesures de protection. Nucleus Research estime que cette perte peut représenter jusqu'à 1 934,00 \$ par année, par employé. De façon plus conservatrice, si on estime le coût de la main-d'œuvre à 20,00 \$ l'heure et qu'on calcule qu'un employé consacre cinq minutes par jour à gérer son pourriel (c'est-à-dire à prendre une décision sur la nature du message et sur son élimination), alors cette tâche représente une perte de productivité d'environ 43,00 \$ par mois par employé. Il est facile de calculer la perte exacte en fonction du volume de pourriel que vous recevez et des salaires en vigueur dans votre organisation.

Calcul de la perte de productivité	Formule	Exemple
Nombre d'employés qui reçoivent du pourriel (A)	A	100
Minutes quotidiennes pour la gestion (B)	B	5
Minutes quotidiennes perdues (C)	A*B	500
Rémunération horaire moyenne (D)	20,00 \$	20,00 \$
Charges sociales (E)	19 %	19 %
Coût du pourriel par jour (F)	$C*(D/60)*(1+E)$	198,33 \$
Coût mensuel du pourriel	F*30	4 363,33 \$

Bande passante (aggravation de la menace)

Environ 85 % des connexions SMTP sont indésirables. La bande passante du lien Internet, congestionnée inutilement, n'est donc pas disponible à pleine capacité pour les applications de commerce électronique, la navigation et tous les systèmes reliés à Internet. Cette situation peut occasionner une dégradation du temps de réponse, la non-disponibilité du réseau pour des applications critiques et éventuellement, amener l'entreprise à chercher à augmenter sa capacité avec de nouveaux liens.

Dans le cas d'une menace aggravée, par exemple, si l'entreprise est victime d'une attaque de dictionnaire, le problème de congestion devient critique. Les requêtes nuisibles peuvent alors saturer complètement la bande passante et engendrer des frais de surcharge de transfert. Il est même possible que les serveurs surchargés ne soient plus en mesure d'assurer la disponibilité du service de courriel. La gravité de la menace ne dépend pas de la taille de l'entreprise. En effet, nous voyons souvent de petites entreprises, qui n'ont que quelques dizaines de boîtes de courriel, aux prises avec des centaines de milliers de connexions malveillantes par jour.

Impact sur les ressources

L'infrastructure de courriel de l'entreprise est lourdement taxée par le pourriel. Chaque pourriel reçu consomme inutilement la capacité de traitement des serveurs entrants, l'espace disque, la bande passante sur le réseau interne et congestionne les serveurs et les postes de travail.

Cette charge inutile peut en venir à demander une mise à niveau des équipements, entraînant ainsi des investissements qui n'auraient dû, normalement, être consentis que beaucoup plus tard.

Les coûts indirects

Les coûts indirects regroupent tous les coûts et inconvénients qui ne peuvent être quantifiés mais qui occasionnent néanmoins inutilement des frais pour l'entreprise.

Les faux-positifs humains

Pour les organisations qui ne possèdent pas de protection antispam ou une protection inefficace, le risque de faux positif humain aussi appelé « *Oups factor* » est occasionné par le destinataire lui-même qui en vient à détruire du courriel légitime à l'intérieur d'une sélection en bloc de plusieurs pourriels. Aussi ironique qu'elle soit, cette situation peut causer la perte de messages de grande importance.

Détresse psychologique

Bien que les conséquences du pourriel pour les employés soient généralement considérées comme plutôt bénignes, certains peuvent avoir de vives réactions s'ils sont constamment exposés à du contenu inapproprié qui heurte leurs valeurs ou leurs croyances. La rumeur veut même que certaines entreprises aient été poursuivies en justice par des employés qui estimaient qu'elles leur avaient fourni un cadre de travail hostile à cause du pourriel. En réalité, la responsabilité des entreprises à cet égard demeure théorique car, selon les informations dont nous disposons, aucune cause de ce genre n'a encore été plaidée devant les tribunaux. Quoi qu'il en soit, on peut penser que les entreprises ont la responsabilité morale de fournir un environnement de travail à l'abri des messages offensants.

Perte de confiance

Le pourriel a comme conséquence générale une perte de confiance dans la fiabilité du courrier électronique. La multiplicité des mesures déployées pour contrer le pourriel et le blocage occasionnel de courriels légitimes ont pour effet de miner la confiance des usagers. Avec toute la panoplie des technologies en place – bonnes et moins bonnes – personne ne peut désormais être assuré qu'un message sera bel et bien livré à destination. Cette conséquence fâcheuse du pourriel pousse certains utilisateurs à se tourner vers une technologie point à point pour les envois critiques : la télécopie. De fait on assiste depuis quelques années à une baisse du taux de livraison du courrier. Il n'existe plus aucune garantie qu'un message expédié par courriel soit effectivement bel et bien livré à son destinataire. Le groupe Lyris, publie à chaque trimestre des données renversantes sur les taux de livraison obtenus auprès des grands fournisseurs de services Internet. Voir www.lyris.com/resources/reports/index.html

Accroissement des coûts pour les envoyeurs massifs

Les grands détaillants sont de gros utilisateurs du courrier électronique. Ils ont compris l'immense impact de ce médium et ont été rapidement séduits par son pouvoir de pénétration et ses coûts d'envois dérisoires. Des entreprises offrant des services d'envois massifs sont apparues sur le marché. Plusieurs grands détaillants ont choisi de

leur sous-contracter le travail d'envoi de courriels, d'autres ont choisies de mener elles-mêmes leurs campagnes de promotion et d'intégrer le courriel à leur stratégie CRM.

Le volume de pourriel qui inonde le marché et l'intolérance grandissante face à cette intrusion viennent cependant modifier la donne pour les envoyeurs de masse. D'une part, les grands détaillants veulent à tout prix éviter d'être perçus comme des polluposteurs et, d'autre part, le barrage des mesures anti-pourriel mine de plus en plus l'efficacité de leurs campagnes promotionnelles.

Pour les envoyeurs massifs, cette situation se traduit par une nette augmentation des coûts de gestion du médium courriel. Les listes d'adresses doivent être strictement contrôlées, il faut obtenir et conserver le consentement du destinataire, le serveur d'envoi ne doit pas congestionner les serveurs des fournisseurs de services, etc. Une négligence à ce niveau et le domaine ou le serveur de provenance pourrait se retrouver sur une liste noire d'envoyeurs, ce qui pourrait non seulement pénaliser la fonction marketing mais compromettre aussi la livraison du courriel pour toute l'entreprise.

En mai 2005, le groupe de travail sur le pourriel mis sur pied par Industrie Canada publiait un rapport contenant plusieurs recommandations visant les envoyeurs massifs. Voici les plus importantes.

- Les courriels de marketing devraient être envoyés uniquement aux destinataires qui ont consenti à recevoir les renseignements.
- Les courriels de marketing doivent fournir aux destinataires un moyen évident, clair et efficace de refuser, par courriel ou Internet, de recevoir d'autres courriels d'affaires et/ou de marketing de l'organisme.
- Le processus interne utilisé pour obtenir le consentement devrait être clair et transparent. Les organismes devraient conserver un dossier des types de demandes reçues des destinataires, afin de pouvoir mettre leurs listes d'envois de courriels à jour avant les campagnes de publicité.
- Chaque communication de marketing par courriel devrait clairement identifier l'expéditeur du courriel. La ligne de mention objet et le corps du texte devraient refléter correctement le contenu, l'origine et le but de la communication.
- Tout courriel devrait fournir un lien vers la politique de l'expéditeur sur les renseignements personnels. Celle-ci devrait expliquer le mode d'utilisation et de communication des renseignements personnels pouvant être recueillis par le biais du parcours de l'utilisateur ou d'autres techniques de surveillance des sites Web.
- Les entreprises de marketing, les courtiers et les propriétaires de listes d'adresses devraient prendre des mesures raisonnables pour s'assurer que les personnes dont l'adresse figure sur leurs listes de diffusion ont donné le consentement approprié.
- Les entreprises de marketing qui font du marketing par courriel auprès des personnes mineures devraient faire preuve de discrétion et de sensibilité et tenir compte de l'âge, des connaissances, du caractère averti et de la maturité de cet auditoire.
- En matière de contenus pour adultes :
 - a) lorsque le contenu d'un courriel est destiné à des adultes, l'expéditeur devrait, avant de l'envoyer, vérifier si le destinataire est en âge de recevoir et de consulter légalement ce contenu
 - b) tout courriel renfermant un contenu sexuellement explicite devrait inclure la balise de préface « SEXUELLEMENT EXPLICITE » dans la ligne de mention objet.

- Les organismes devraient mettre en place un système de traitement des plaintes juste, efficace, confidentiel et facile à utiliser.
- Les organismes peuvent divulguer les adresses de courriel de leurs clients à des tiers affiliés ou au sein d'une famille de sociétés si :
 - a) ils ont obtenu leur consentement;
 - b) ils utilisent les adresses aux fins pour lesquelles ils les ont recueillies (c'est-à-dire pour un marketing relié à l'achat original ou à la prestation de services associés à cet achat);
 - c) les destinataires savent pourquoi ils reçoivent des courriels;
 - d) il y a un moyen facile de refuser de recevoir davantage de courriels.

Source : e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/h_gv00317f.html

LES TECHNIQUES DE BLOCAGE

Quels que soient les outils utilisés, les techniques de lutte contre le pourriel sont clairement définies et bien connues, même si elles se raffinent constamment. En fait, la plupart des solutions de filtrage commerciales utilisent une combinaison de techniques car il a été démontré que la multiplication des techniques de détection utilisées augmente l'efficacité du filtrage.

Enveloppe ou contenu?

Les informations d'enveloppe sont les informations échangées entre les serveurs de courriel pour assurer la livraison des messages d'une machine à une autre. Ces informations comprennent l'adresse courriel de l'expéditeur, l'adresse du destinataire, l'adresse IP de l'expéditeur et sa bannière de présentation (*HELLO banner*) lors d'une connexion SMTP. Ces informations constituent ce qu'on appelle les en-têtes des messages. Ce sont elles qui permettent de reconstituer, dans une certaine mesure, le routage du courriel.

Le terme « contenu » désigne le corps du message, que celui-ci soit constitué de texte brut, de texte en format HTML ou de documents joints comme des images ou d'autres types de fichiers.

Vous pouvez rejeter certains envois postaux sans même les ouvrir. De la même manière, il est aussi possible de rejeter des courriels sans en inspecter le contenu. Cette approche est moins coûteuse en ressources machine et peut permettre de rejeter jusqu'à 70 % du volume de courriel entrant. L'économie vient du fait que si, lors d'une connexion SMTP, on peut détecter rapidement la nature indésirable d'une communication, on pourra y mettre fin sans avoir à traiter le contenu. En effet, le traitement du contenu est plus complexe et exige davantage de ressources. Ce rejet qui intervient entre la connexion et la communication du message s'apparente un peu au geste de raccrocher le téléphone pour éviter un appel de sollicitation lorsqu'on détecte le petit délai induit par les composeurs automatiques.

Techniques de blocage agissant au niveau enveloppe

Listes noires

La première technique de blocage est la constitution de listes noires de domaines ou d'adresses IP nuisibles. Tous les envois provenant de ces domaines ou adresses IP sont systématiquement bloqués.

Cette technique est la plus ancienne mais elle est aussi la plus lourde à maintenir. En outre, elle n'est d'aucun recours contre les polluposteurs qui opèrent depuis des « *botnets* » car les informations d'enveloppe des courriels envoyés par ces réseaux de zombies sont en mutation perpétuelle. Qui plus est, les polluposteurs ont appris depuis longtemps à danser avec les noms de domaine et les adresses IP.

Les Rbls (Real time blackhole lists) ou DNSbl (DNS blackhole lists)

Les listes de blocage DNS sont constituées et mises à jour par des organismes externes qui se sont donné le mandat d'accomplir cette tâche gratuitement et pour le bien commun. Ces organismes utilisent le système DNS comme base de données pour mettre en place un système dynamique qui vérifie si l'expéditeur se trouve sur l'une des listes noires dont ils disposent. Ces listes sont établies selon des critères variables, déterminés par l'administrateur du Rbl. À l'origine, elles étaient basées surtout sur la détection de relais ouverts. Les relais ouverts sont des machines qui acceptent de retransmettre un message vers un domaine qui ne constitue pas leur destination finale. Ils sont utilisés comme tremplins pour l'envoi massif de pourriel. Avec un Rbl, une passerelle de réception est en mesure d'identifier une source malveillante à l'aide d'une simple requête DNS. Plusieurs plateformes de courrier électronique, comme MS-Exchange®, Sendmail et Lotus Notes/Domino® supportent maintenant les services DNSbl.

Chaque service DNSbl établit ses propres critères d'inscription et sa politique de rectification. Il existe des centaines d'opérateurs de services DNSbl qui identifient des relais ouverts, des adresses IP dynamiques, des réseaux de polluposteurs connus, des plages d'adresses de liens commutés, d'adresses IP dynamiques, des serveurs hors normes, etc. Le choix est vaste et, pour l'utilisateur, la principale difficulté consiste à choisir le bon service.

Discussion :

Les listes noires maintenues par des organisations comme Spamhaus, Spews et Spamcop sont assez efficaces et devraient faire partie de l'arsenal anti-pourriel de base de toute entreprise. Ces listes comportent un faible risque de faux positifs - les expéditeurs listés injustement - mais leur efficacité, qui peut atteindre 70 %, justifie amplement leur emploi. Ces services publics de listes noires présentent l'immense avantage de couper la communication avant que le corps du message ne commence à être reçu par le serveur. Les DNSbl sont cependant inefficaces pour contrer le pourriel envoyé depuis les « *botnets* » qui naissent et meurent quotidiennement et pour lesquels on estime qu'ils émettent 60% du spam total sur la planète. Dans le cas des serveurs sous haute charge, l'utilisation de DNSbl générera un grand nombre de requêtes DNS qu'il faudra réduire, par exemple, avec un transfert de zone local.

Ce qui est important de retenir au sujet des services DNSbl, c'est que ni l'efficacité ni la précision de leur filtrage ne sont entre les mains du client. En effet, celui-ci n'exerce aucun contrôle sur cette tâche. Il faut aussi garder à l'esprit que ces organismes peuvent disparaître du jour au lendemain et que le filtrage devient intrinsèquement dépendant du service DNS.

Un répertoire assez complet des services positifs est disponible à www.spamlinks.net/filter-dnsbl-lists.htm

SPF et DKIM

Le système SPF (« Sender Policy Framework » : www.openspf.org) se base sur la déclaration des adresses IP valides des serveurs de courriel sortants autorisés pour un domaine donné. Ainsi, un serveur doté d'un client SPF est en mesure de vérifier que le courriel d'un domaine provient bel et bien des serveurs déclarés légitimes pour ce domaine et de le bloquer si ce n'est pas le cas. SPF est gratuit et peut être adopté par toute organisation. Il suffit, pour ce faire, d'inscrire un enregistrement DNS approprié. Les systèmes SPF qui vérifient l'intégrité des informations sont généralement des ajouts ou des modules ajoutés aux plateformes de courriel.

Discussion :

SPF et SenderID sont des solutions qui visent davantage à protéger l'intégrité d'un domaine qu'à réellement bloquer le pourriel. En effet, rien n'empêche un polluposteur d'inclure une zone SPF légitime pour le domaine qu'il utilise pour le pollupostage. De fait environ 16% des messages nuisibles proviennent d'un domaine avec une mesure SPF. Cette mesure a néanmoins l'avantage de protéger les domaines couramment usurpés pour l'envoi de pourriel comme Yahoo, MSN, Hotmail, etc.

DKIM (« Domain Keys Identified Mail ») est une nouvelle norme élaborée par Cisco® et Yahoo® au cours de l'été 2005. Elle encadre l'utilisation de signatures numériques pour l'authentification tant du contenu que des informations d'enveloppe associées à des domaines Internet.

Disponible gratuitement, cette technologie, à laquelle Microsoft souscrit, utilise le système DNS pour la diffusion de clés publiques et n'impose aucune modification des logiciels clients (MUA) comme Outlook, Notes ou Thunderbird.

En clair, DKIM permet de garantir que l'expéditeur d'un message est effectivement autorisé et considéré comme un expéditeur légitime pour ce domaine et que le contenu du message est intègre. Une signature chiffrée générée à partir des entêtes et du contenu est insérée dans une entête à cette fin.

DKIM est une norme en devenir. À l'heure actuelle, cette approche n'est supportée que par un petit nombre de plateformes de courriel et vise surtout les gros expéditeurs. Google utilise DKIM pour son service gmail. Utilisés conjointement, DKIM et SPF vont permettre à l'avenir plus de vérifications d'intégrité dans la transmission du courriel. DKIM et SPF ne sont cependant pas des systèmes d'accréditation ou de réputation. Ils apportent une solution intéressante au problème des messages forgés avec de fausses adresses mais ils n'empêchent en rien les polluposteurs d'opérer avec leurs propres domaines d'envoi.

Ceci dit, la publication d'une mesure SPF est une excellente façon de contrer le problème des tempêtes d'avis de non livraison (« *DSN Backscatter* ») où un nom de domaine est usurpé et où son propriétaire légitime reçoit un déluge de messages de rejet.

Intégrité SMTP

Un nombre considérable de messages peuvent être rejetés simplement en imposant certaines règles d'intégrité lors du dialogue SMTP. En voulant brouiller les pistes, les polluposteurs vont volontairement falsifier leur adresse IP, le nom d'hôte ou celui de la bannière de connexion. Par exemple, il est tout à fait légitime d'exiger une bannière de connexion valide et de rejeter les messages en provenance de *127.0.0.1* (adresse locale) ou encore les messages provenant de l'adresse IP du serveur de réception, d'une adresse IP dynamique ou encore de noms réservés comme *localhost* ou *localhost.localdomain*.

Pour être en mesure de recevoir du courrier électronique, tout domaine doit avoir un enregistrement MX ou une entrée A valable inscrite au système DNS. Cette information indique à toute la planète quel serveur est responsable de la réception du courriel pour ce domaine. Il est donc acceptable de rejeter les messages en provenance d'un domaine pour lequel il n'existe aucune entrée MX au DNS, c'est-à-dire un domaine qui n'est pas lui-même en mesure de recevoir du courriel.

Certaines règles d'intégrité peuvent être définies localement. Par exemple, un serveur pourrait implanter une politique de rejet basée sur un test qui vérifie si le nom d'hôte du client SMTP est bel et bien associé au domaine déclaré par l'expéditeur.

Discussion :

Le protocole SMTP a été créé par feu John Postel en 1982 (www.rfc-editor.org/rfc/rfc821.txt), bien avant l'explosion d'Internet. L'objectif de ce protocole était d'assurer une livraison maximale. Les préoccupations actuelles sur l'utilisation malveillante du courriel étaient alors inexistantes.

C'est pourquoi aucune mesure d'intégrité stricte ne fait partie de la définition du protocole. L'ajout ad hoc de contraintes peut compromettre la livraison du courriel légitime. Par exemple, il est possible de rejeter le courriel d'un client SMTP si aucun nom d'hôte ne correspond à son adresse IP (rDNS) mais cette règle pénalisera un grand nombre de serveurs mal configurés qui ne possèdent pas d'entrée rDNS.

Les serveurs de courriel (MTA) qui permettent d'exercer un bon contrôle des règles d'intégrité vont pouvoir éliminer sans efforts un volume important de pourriel sans consommer trop de ressources. Ces dispositions seront spécialement importantes pour les serveurs à haut volume.

Les règles d'intégrité SMTP sont d'un précieux secours mais il importe de bien comprendre leur impact sur l'infrastructure de courriel en place.

Il existe un Rbl qui identifie les serveurs ne respectant pas intégralement les normes établies sur Internet. Ce service peut certes être utile, mais il faut savoir que plusieurs serveurs commerciaux utilisent leur propre version modifiée du protocole SMTP, version qui n'est pas

nécessairement conforme aux norme établies. En outre, sur Internet, rien n'oblige un serveur à se conformer strictement aux protocoles établis. Voir : www.rfc-ignorant.org

Le contrôle de débit

Le contrôle de débit vise à pénaliser un envoyeur dont le volume d'envois dépasse un certain niveau ou alors si la proportion de rejets dépasse un seuil déterminé. Dans le dernier cas on parle alors de contrôle de débit selon la réputation (« *Reputation based flow control* »). Cette approche basée sur la réputation (bonne ou mauvaise) permet un pouvoir discriminant plus fort que sur la simple identité comme c'est le cas avec les listes noires ou les DNSbl. La technique permet de se baser sur des informations objectives comme le nombre de rejets, les plaintes reçues ou la réception en provenance d'adresses leurrées. Plusieurs variantes de contrôle de débit existent mais elles ont toutes l'avantage d'agir au niveau de l'enveloppe et de pouvoir intercepter plus de 50% des connexions malveillantes. Ironport maintient un registre public sur les volumes d'envois et la réputation disponible à www.senderbase.org. On assiste maintenant à l'émergence d'un véritable marché pour les évaluateurs de réputation ou RSP « *Reputation service Providers* ».

Le « greylisting »

Le « *greylisting* » est une technique d'évitement et non une technique de filtrage. Cette approche permet d'identifier les envoyeurs malveillants en fonction de leur comportement lors d'une session SMTP. La technique ralentit le débit du service pour les envoyeurs inconnus en introduisant une réponse de non-disponibilité temporaire formulée comme suit : « 421 - Temporary failure ». Les serveurs correctement configurés vont tout simplement retransmettre le message un peu plus tard alors qu'un « *Spamware* » passera à la prochaine adresse de la liste, sans tentative de retransmission. Si le polluposteur choisit malgré tout de retransmettre le message, il s'expose alors à des délais de transmission qui compromettront sérieusement l'efficacité de son opération.

L'inconvénient du « *greylisting* », c'est qu'il induit un léger délai dans la livraison du courriel. Lorsque les logiciels serveurs sont mal configurés ou qu'ils ne respectent pas le protocole SMTP, ce délai peut même compromettre la livraison. Le « *greylisting* » exige d'importantes ressources mémoire; il doit donc être implanté avec le plus grand soin sur les serveurs à haut volume.

Techniques de blocage agissant au niveau enveloppe

Le filtrage de contenu comprend toutes les techniques qui se basent sur le contenu pour prendre une décision sur la nature nuisible d'un message. Le filtrage de contenu est essentiel pour atteindre une efficacité supérieure à 95 %. À lui seul, le filtrage d'enveloppe ne peut atteindre un niveau d'efficacité assez élevé pour être considéré comme une protection valable.

Un mot sur le camouflage du contenu

À cause de la profusion et de la variété des techniques de détection, un grand nombre de stratagèmes ont été créés pour camoufler le contenu des courriels. Certains d'entre eux sont risibles alors que d'autres sont remarquablement efficaces. L'une des techniques qui a déjà été utilisée est celle du texte en tableau. Le texte est décliné verticalement, ce qui déjoue bon nombre de filtres tentant d'agir sur les mots.

```
v c v  
i i a  
a a l  
g l i  
r i u  
a s m
```

La référence la plus complète en matière de camouflage est sans aucun doute le « *Spammer's Compendium* », colligé et tenu à jour par John-Graham Cummings à l'adresse www.jgc.org/tsc/

Les mots clés – une technique à proscrire

La pire méthode de filtrage est celle qui se base sur la présence de mots clés. Cette méthode, l'une des premières et probablement la plus intuitive, génère un taux élevé de faux positifs et peut facilement être déjouée au moyen de variations d'orthographe infinies. Cette technique est hautement réactive et exige un effort de gestion important.

Les expressions régulières

Les expressions régulières sont des formules qui permettent d'intercepter des contenus malgré certaines variations de format déterminées. Par exemple, l'expression régulière « `/(?i)[vi]+[gra]/` » va filtrer tous les mots qui commencent par « vi » et se terminent par « gra ».

Les expressions régulières sont surtout utiles pour déceler les techniques de camouflage de contenu. Elles permettent d'identifier facilement les courriels dont les URL de destination comportent des codes hexadécimaux ou des adresses IP. La maintenance des règles constitue l'inconvénient principal de cette technique. Il existe cependant certains sites qui développent des expressions régulières adaptées sur une base continue.

Les heuristiques – Spam Assassin

Le filtrage heuristique regroupe toutes les techniques qui analysent différentes caractéristiques du message. Ainsi, avant qu'une décision ne soit rendue sur la nature d'un message, plusieurs caractéristiques seront examinées et un poids relatif sera attribué à chaque caractéristique positive. Spam Assassin est un référentiel qui permet d'intégrer les règles heuristiques dans un système de pointage adapté. Chaque test positif correspond à un pointage sur l'échelle

d'identification du spam et le total obtenu en additionnant le pointage de tous les tests permet de prendre une décision sur la nature nocive de l'envoi. La plupart du temps les caractéristiques sont évaluées à partir d'expressions régulières sur des portions de contenu.

Par exemple :

```
Delivered-To: user@zerospam.ca
X-Envelope-From: <ZYSTUQYOTN@browniesnyc.com>
X-Quarantine-id: <spam-af7e924cf0ec2caad99cc9bc8fd-20051225-013319-09611-05>
Received: from 209.172.38.68 (unknown [61.1.225.131])
    by filter.zerospam.ca (Postfix) with SMTP id 6448C2053EC
    for <user@zerospam.ca>; Sun, 25 Dec 2005 01:33:03 -0500 (EST)
Received: from .starnetusa.net (.starnetusa.net [1])
    by .starnetusa.net with ESMTP id 2C573160
    for <ZYSTUQYOTN@browniesnyc.com>; Sun, 25 Dec 2005 10:29:25 +0400
Message-Id: <6.7.7.13.2.20031533103053.025b4b48@.starnetusa.net>
X-Sender: ZYSTUQYOTN@browniesnyc.com (Unverified)
X-Mailer: QUALCOMM Windows Eudora Version 6.0.0.22
Date: Sun, 25 Dec 2005 07:26:25 +0100
From: "Mickey Bain" <ZYSTUQYOTN@browniesnyc.com>
To: user@zerospam.ca
Subject: Your services about to be canceled
X-Spam-Status: Yes, hits=12.3 tag1=-1000.0 tag2=4.0 kill=4.0 tests=BAYES_50,
```

```
DCC_CHECK, FUZZY_ERECT, INFO_TLD, RCVD_HELO_IP_MISMATCH, RCVD_NUMERIC_HELO
```

"Ci-iallis Sof-tabs" is better than Pfizer V-iiaggrra and normal Ci-ialis because:

- Guarantes 36 hours lasting
- Safe to take, no side effectts at all
- Boost and increase se-xual perfoormance
- Haarder e-rectiitions and quick recharge
- Proven and c-ertified by e-xperts and d-octors
- only \$1.98 per tabs
- Special offeer! These prices
- are valid u-ntil 30th of December !

Cllick hereee: <http://hadanopc.info>

Exemple de tests heuristiques effectués par Spam Assassin

L'analyse des résultats de plusieurs sites utilisant Spam Assassin suggère qu'un petit nombre de règles réussissent à filtrer un grand nombre de pourriels. Le principe du 80/20 semble s'appliquer à la validité ou à l'utilité des règles d'analyse heuristique. SpamAssassin est le référentiel heuristique le plus utilisé, tant pour des produits commerciaux que pour des solutions maison. Il faut savoir que spamassassin constitue le tout premier test avec lequel les polluposteurs intelligents valideront leurs campagnes.

Le filtrage statistique – Bayes / CRM114 / DSPAM

Cette technique requiert la construction d'une base de plusieurs milliers de pourriels et de courriels légitimes. C'est ce qu'on appelle les corpus de SPAM et de HAM. Le contenu de chaque nouveau courriel est analysé et le texte est découpé en chaînes. Ces chaînes sont comparées avec le contenu des corpus de SPAM et de HAM et c'est la fréquence de leur apparition dans l'un ou l'autre des corpus qui détermine leur classement. On calcule cette fréquence en utilisant une formule élaborée par le statisticien Bayes et on obtient alors un nombre correspondant à la probabilité que le courriel soit un pourriel. On peut alors déterminer le seuil au-delà duquel les courriels seront considérés comme du spam.

À ses débuts, le filtrage statistique donnait des résultats exceptionnels; son efficacité pouvait atteindre 99 %. Les polluposteurs se sont cependant vite adaptés à cette approche et ils ont mis au point des mesures pour la contourner. L'une de ces mesures est l'injection de prose. L'envoyeur insère dans son message des portions de texte aléatoires, souvent puisées dans la littérature. Ces portions de texte n'ont absolument aucun lien avec le message mais leur ajout a pour effet de réduire le poids statistique des chaînes incriminantes et peut éventuellement déjouer le filtre statistique. Le filtrage statistique est aussi mal adapté au spam envoyé sous forme d'image contre lequel il est impuissant. Malgré ses faiblesses, cette technique se raffine sans cesse et a probablement plus d'avenir pour innocenter le courriel légitime que pour identifier le spam.

C'est lorsqu'il est adapté à des profils de courriel individuels que le filtrage Bayésien est le plus efficace. La technique parvient alors à cerner assez précisément les vocabulaires personnels des messages qui constituent du pourriel et du courriel légitime. Outlook 2003 et Thunderbird intègrent maintenant le filtrage Bayésien.

Filtrage d'URL

Les polluposteurs travaillent tous dans le même but : déclencher une action, comme par exemple amener la victime à cliquer sur un lien. Il leur faut donc inclure un lien de destination dans le message. Le filtrage des URL contenus dans les messages est l'une des techniques les plus efficaces. Dans le cadre de cette approche, on utilise l'infrastructure des Rbl pour tenir à jour des listes noires d'adresses de sites (URLs) figurant dans les messages. Peu coûteuse, cette technique permet des taux de détection entre 40% et 60 %. Détails www.surbl.org

Le pourriel sur les actions (« *Pump and dump spam* ») qui utilise à la fois une image et qui contrairement aux autres formes de spam, n'inclut pas d'URL dans le message, est très bien parvenu à déjouer cette technique. On assiste aussi à la naissance d'engins de pollupostage qui sont en mesure d'utiliser des milliers d'URL différents mais ayant tous la même destination.

Les signatures – RAZOR / PHYZOR / DCC

Certaines organisations accumulent des échantillons de pourriel dans le but de créer des bases de signatures avec lesquelles les messages reçus pourront être comparés. S'il y a correspondance, on pourra alors rejeter le message.

Par exemple, dès que le système RAZOR reçoit un nouveau spécimen de pourriel, il lui attribue une signature unique (le CRC), qui correspond très exactement à son contenu. Les serveurs clients peuvent ensuite faire appel au système RAZOR afin de vérifier dynamiquement la signature des courriels entrants et rejeter ceux qui correspondent aux signatures de la base. Les signatures sont de plus en plus perfectionnées et sont maintenant capables d'intercepter des courriels dans lesquels des variations subtiles de contenu ont été insérées dans le but de déjouer la détection. Certaines bases de signatures comme Razor et DCC sont gratuites alors que d'autres sont exploitées sur une base commerciale.

Le phénomène du spam sous forme d'image a bonifié l'utilité des bases de signatures. Les fournisseurs commerciaux comme Cloudmark™ et Commtouch™ sont parvenus à générer des signatures floues qui peuvent identifier des variantes polymorphiques d'un même message. Les signatures de contenu sont en fait les seules méthodes capables d'identifier avec un haut degré de certitude les cas de spam image.

Comme c'est le cas pour les Rbl, le hic avec l'utilisation de systèmes de signatures comme base de détection, c'est que l'utilisateur s'en remet à l'efficacité des algorithmes de détection, à la profondeur du réseau et à la disponibilité d'un tiers et que ceux-ci agissent essentiellement après le fait.

Les « SVM Support Vector machine »

Ces solutions sont les plus avancées mais aussi les plus complexes. Elles utilisent une technique de reconnaissance basée sur l'apprentissage machine. À cause de leur complexité, peu de systèmes les utilisent mais elles semblent présenter un grand potentiel.

LES STRATÉGIES DE FILTRAGE

En matière de sécurité du courriel, toutes les solutions de filtrage se classent dans l'une des trois grandes catégories suivantes : les **solutions clients**, les **solutions passerelles** ou les **solutions en amont**. Tous les systèmes de filtrage commerciaux, de même que les systèmes provenant du monde du logiciel libre utilisent une savante combinaison des techniques de filtrage présentées plus haut. Les meilleurs produits sont ceux qui intègrent une grande variété de techniques complémentaires car cette approche augmente leur taux d'efficacité.

a) Les solutions client

Ces solutions passent par l'installation de logiciels sur le poste de travail du client dont on veut protéger la boîte de courriel. Bien qu'acceptables pour les micro entreprises (de un à trois postes de travail), ces solutions deviennent rapidement inadéquates pour les plus grands réseaux. En plus d'être coûteuses, elles doivent être déployées sur tous les postes et leur maintenance suppose aussi des efforts de soutien technique. Mais leur plus grand handicap, c'est surtout le fait qu'elles interviennent en bout de piste, après que le pourriel

ait été reçu et qu'il ait consommé la bande passante, les ressources de traitement et l'espace disque. Par ailleurs, ces solutions ne peuvent profiter des techniques de filtrage d'enveloppe car elles interviennent après que le courriel ait été reçu et accepté par la passerelle de réception.

Les produits commerciaux disponibles sont innombrables mais la plupart d'entre eux visent surtout la clientèle résidentielle.

b) Les solutions passerelles

Les solutions de type passerelle sont déployées dans le périmètre réseau de l'entreprise autour du serveur de courriel entrant. Il peut s'agir de solutions logicielles intégrées ou non au serveur ou encore d'appareils dédiés agissant comme hôtes de bastionnage.

Sécurité

Comme c'est le cas chaque fois qu'on ajoute un élément dans l'infrastructure informatique d'une entreprise, il faut prendre soin de bien évaluer la sécurité des nouveaux systèmes, surtout celle des systèmes de protection. Qu'advierait-il de la confidentialité de vos courriels si la plateforme de protection était compromise? En 2005, on a découvert plus de vulnérabilités dans les systèmes de sécurité que dans les systèmes d'exploitation eux mêmes.

Dans le cas des solutions logicielles, c'est l'entreprise utilisatrice qui est responsable du durcissement et de la sécurité de son serveur. Elle doit donc y employer du personnel qualifié pour comprendre et gérer les divers éléments de sécurité et faire enquête en cas d'incident. Il lui faut aussi constamment surveiller la sécurité et être à l'affût des tentatives d'intrusion. Dans le cas des appareils dédiés ou boîtes noires, la sécurité du système de courriel devient tributaire des normes du fabricant. L'utilisation d'une boîte noire procure souvent un faux sentiment de sécurité. En effet, on a constaté que ces appareils peuvent introduire des vulnérabilités importantes et qu'il faut les tenir à jour scrupuleusement.

Il est très important de s'assurer que la solution choisie est assortie d'une garantie que les courriels ne seront pas enregistrés ou archivés sous une forme ou sous une autre et que le fournisseur n'y a pas accès.

Mises à jour

Toute solution sérieuse comporte obligatoirement un abonnement à un service de mise à jour qui permet d'actualiser la solution. Ce service suppose qu'un tiers pourra accéder au périmètre réseau de l'entreprise. C'est sa responsabilité de s'assurer qu'aucune vulnérabilité ou fuite d'information ne puisse circuler sur ce canal privilégié. On est aussi en droit de se questionner au sujet des informations échangées par les agents de mise à jour.

Coûts en capital

Les solutions matérielles et logicielles sont attrayantes par leur coût en apparence peu élevé. Par exemple, certaines solutions n'exigent qu'une licence par appareil, sans égard au nombre d'utilisateurs ou de boîtes postales. Mais elles entraînent des coûts cachés importants. En plus de leur coût d'acquisition, elles exigent des ressources en gestion de projet, en administration de système, en sécurité et, vraisemblablement, en formation des utilisateurs ainsi qu'en soutien technique. Elles occupent aussi de l'espace dans le centre de données, elles nécessitent des ports d'accès, une alimentation électrique protégée, elles entraînent des frais d'entretien et exigent parfois la mise en place d'un dispositif de sauvegarde. Une bonne protection contre les défaillances possibles passe aussi par la redondance, c'est-à-dire l'ajout d'un deuxième appareil, ce qui multiplie par deux les coûts d'acquisition et les frais d'exploitation.

Un seul MX protégé

Les utilisateurs de solutions passerelle font souvent l'erreur de définir un seul enregistrement MX pour la passerelle protégée. Si le service réseau est interrompu pour ce MX, la livraison du courriel est alors compromise. Il est important de se protéger contre ce genre de situation.

Comme mesure préventive, on configurera un deuxième enregistrement MX, préférablement sur un réseau distinct. De cette façon, en cas de défaillance de la passerelle principale, la réception du courriel sera quand même assurée. Les polluposteurs ont l'habitude de passer par le MX de moindre importance car ils savent qu'il est souvent moins bien protégé sur un réseau distinct. C'est la raison pour laquelle il est essentiel de s'assurer que tous les MX définis offriront le même niveau de protection que la passerelle de destination.

Consommation des ressources

Aucune solution passerelle ne règle le problème du gaspillage de la bande passante où environ 90% du trafic est nuisible. Avec ce type de solution, toutes les connexions malveillantes continuent d'atteindre le périmètre réseau. Si le domaine fait l'objet d'une menace aggravée (DDOS ou DHA), il est possible que l'entreprise soit forcée de faire une mise à niveau vers un appareil ou un serveur plus puissant afin d'être en mesure de traiter la surcharge.

Exemples de solutions logicielles :

- Vircom ModusGate
- GFI Mail Essentials
- Sybari SPAM defense
- Sophos PureMessage

Exemples de solutions matérielles :

Barracuda Spam Firewall
Symantec Mail Security
F-Secure Messaging Gateway
Ironport
Panda GateDefender

c) Les solutions en amont

Les solutions en amont filtrent le contenu indésirable avant qu'il n'atteigne le périmètre réseau. Elles impliquent le changement du pointeur MX vers un ou plusieurs serveurs d'une entité externe. Le fournisseur se charge alors du filtrage du pourriel. Généralement, il offre aussi une protection anti-virus de premier niveau. Une fois le nettoyage terminé, les messages légitimes sont redirigés vers la passerelle de réception de l'entreprise.

Cette approche présente plusieurs avantages. Tout d'abord, elle peut être déployée très rapidement car sa mise en œuvre est complètement indépendante de l'infrastructure informatique de l'organisation, quelles que soient sa nature ou sa complexité. Ensuite, les solutions en amont réduisent le risque financier lié à la protection du courriel car tous les coûts directs et indirects liés à ce type de solution sont connus. Le niveau de sécurité des solutions de filtrage en amont varie selon le prestataire choisi. Les prestataires qui opèrent avec un seul centre de données sont plus vulnérables car, en cas de catastrophe ou de perte de connectivité, aucun centre ne prend la relève. Les prestataires qui utilisent plusieurs centres de données peuvent mitiger ce risque et assurer une meilleure fiabilité du service grâce à la redondance des éléments de transport.

Exactement comme dans le cas des appareils dédiés, le niveau de sécurité de la solution dépend de la qualité du travail du fournisseur, sauf que, dans le cas des solutions en amont, le risque se situe quand même à l'extérieur du périmètre réseau de l'entreprise. Il importe néanmoins de bien l'évaluer et de s'assurer, par exemple, que les installations où sont hébergés les systèmes du fournisseur sont suffisamment protégées et que la sécurité y est gérée sérieusement. Il faut aussi vérifier si le fournisseur offre une véritable redondance réseau et si ses systèmes sont surveillés sur une base continue.

Dès leur mise en œuvre, toutes les solutions imparties ont l'avantage de réduire la consommation de la bande passante attribuable aux envois nocifs. À l'heure actuelle, cette réduction est de l'ordre de 70 à 90 % et varie en fonction du « bruit » circulant sur le réseau. Dans le cas d'une menace aggravée, cette économie peut être encore plus élevée.

En ce qui concerne la confidentialité, on devra s'assurer que le fournisseur offre des garanties écrites et qu'il ne conserve aucun message sur ses systèmes.

Comme c'est le cas pour beaucoup de services impartis, une bonne part du succès du filtrage en amont réside dans la confiance qui peut être établie entre le client et le prestataire de services. La crédibilité du fournisseur, sa réputation, le nombre d'incidents qu'on lui attribue et les références de ses clients sont des facteurs décisionnels non techniques mais tout aussi importants.

Le tableau ci-dessous résume les avantages et inconvénients liés à chaque type de solution.

Intérieur du périmètre	Périmètre réseau		Extérieur du périmètre
Solutions client	Passerelles HW / SW	Appareils dédiés	Services impartis
A V A N T A G E S			
<ul style="list-style-type: none"> - Adaptées pour 1 à 5 usagers 	<ul style="list-style-type: none"> - Contrôle de l'environnement - Contrôle de la sécurité 	<ul style="list-style-type: none"> - Déploiement simple - Protection anti-virus - Coûts fixes 	<ul style="list-style-type: none"> - Redondance - Dim. de la charge - Toujours à jour - Aucune gestion - 0 impact sur infrastr. - Déploiement rapide - Économie de band. pass. - Protection virale de niv. 1 - Protection du réseau contre les DDOS
I N C O N V É N I E N T S			
<ul style="list-style-type: none"> - \$ d'acquisition élevés - Serveurs taxés - Déploiement difficile non applicable > 10 - Efficacité mitigée 	<ul style="list-style-type: none"> - \$ capital élevés - \$ bande passante - \$ maintenance - Administration - Intégration infrastr. - Durcissement - Surveillance et mises à jour 	<ul style="list-style-type: none"> - \$ capital élevés - \$ bande passante - Administration - Intégration infrastr. - Dépendance fourn. - Capacité de croître avec les besoins - Fiabilité ? - Pas de redondance - Divulgation 	<ul style="list-style-type: none"> - Confiance du tiers - Sécurité du tiers - Trafic trans-frontalier ? - Confidentialité garantie ?

LA LOI

Contexte américain

Le « *CAN-SPAM Act* », qui fut adopté par le Congrès américain en janvier 2004, est la principale législation visant spécifiquement le pourriel en Amérique du Nord. Cette loi n'interdit pas les envois non sollicités mais elle exige simplement qu'un expéditeur fournisse un lien ou une méthode de désabonnement. C'est ce qu'on appelle le « *opt-out* ». Cette loi a été sévèrement critiquée, principalement à cause du fait que la base de son application est jugée insuffisante.

Depuis l'adoption du *CAN-SPAM Act*, le taux de pourriels circulant sur Internet est passé de 45 % (janvier 2004) à près de 80 % (hiver 2005). Depuis 2007, le niveau de pourriel s'est stabilisé autour de 90 %. Les spécialistes ne pensent pas que cette loi ait vraiment découragé les polluposteurs. À preuve : leur base d'envoi est encore largement située aux États-Unis, même si elle a pris de l'ampleur en Chine et en Corée.

En rendant le « *opt-out* » obligatoire la loi a instantanément légitimé la pratique du pollupostage. Pour opérer légalement, les polluposteurs n'ont qu'à fournir un lien de désabonnement. C'est ainsi que les utilisateurs de courriel se sont retrouvés face un dilemme qu'ils ne peuvent résoudre : comment faire la différence entre un lien de désabonnement éminemment nocif qui, une fois cliqué, multipliera les pourriels qui leur seront envoyés et un lien légitime provenant d'un détaillant en ligne? L'Internaute moyen ne dispose pas des connaissances requises pour faire la différence entre les deux et c'est là le talon d'Achille de cette loi.

La loi a cependant eu des effets positifs, et, dans son rapport de décembre 2005 au Congrès (voir : www.ftc.gov/reports/canspam05/051220canspamrpt.pdf). Le rapport souligne que la loi a eu pour effet d'établir de bonnes pratiques, qui sont maintenant généralement suivies par les expéditeurs légitimes. Elle a aussi établi un cadre légal qui a quand même permis de citer une cinquantaine de cas devant les tribunaux jusqu'à maintenant. Le rapport reconnaît toutefois le rôle qu'a joué l'adoption massive des technologies anti-pourriel dans la réduction récente du volume de pourriel en circulation. En fait, on peut supposer que c'est la baisse du taux de réponse aux campagnes de pollupostage qui diminue l'attrait de cette activité, sans compter que les mesures technologiques de blocage rendent aussi sa pratique de plus en plus complexe.

Contexte européen

L'Union européenne a adopté dès juillet 2002 la directive 2002/58/CE, qui demande aux pays membres d'adopter les dispositions sur le « *opt-in* », aussi appelé « consentement actif ». Le principe de base ayant motivé cette directive est que l'envoi est non désirable s'il n'a pas été sollicité et si le destinataire n'y a pas explicitement consenti. Les différentes lois adoptées par les états membres font cependant l'objet de différences d'interprétation, ce qui complique leur application dans le cas des envois transfrontaliers.

Bien qu'initialement perçue comme ayant plus de mordant que le *CAN-SPAM Act* américain, la directive 2002/58/CE n'a pas amené un grand nombre de condamnations dans les pays signataires. Un homme d'affaires britannique a toutefois réussi à utiliser les dispositions légales européennes pour obtenir d'un polluposteur un règlement hors cours d'une valeur de £300 (voir : www.theregister.co.uk/2005/12/29/uk_spam_win/), ce qui laisse présager que d'autres poursuites sont à prévoir.

Contexte canadien

Au Canada, il n'existe pas encore de cadre juridique s'appliquant spécifiquement au pourriel. Le groupe de travail d'Industrie Canada a déposé son rapport en mai 2005. Celui-ci concluait que « *les lois actuelles ... ne permettent pas, individuellement ou ensemble, d'atteindre l'Objectif global qui est de décourager les polluposteurs au Canada* ».

Ainsi, l'absence de cadre juridique spécifique a pour effet pratique d'empêcher toute poursuite civile ou criminelle sur la base de la seule réception du pourriel. Aucun projet de loi en ce sens n'a encore été déposé à la Chambre des communes.

De l'avis de tous les experts, la législation n'est pas une panacée, même si elle peut avoir un effet dissuasif sur les polluposteurs locaux car, même s'il existait une législation sévère, les réseaux internationaux continueraient d'opérer en toute impunité depuis des pays tiers, parfois complaisants, où il existe encore un vide juridique.

Pour être efficace, la lutte au pourriel exige donc une approche multi-facettes qui englobe non seulement la législation, mais aussi les mesures technologiques, la volonté des entreprises de se conformer, les entreprises de bonnes pratiques commerciales, la coopération internationale et l'adoption de normes favorisant l'authentification des envoyeurs. Le site www.spamlaws.com maintient des liens sur les diverses législations nationales sur le spam.

CONCLUSION

Bien que le niveau d'activité des polluposteurs tende à se stabiliser, le pourriel demeure une réalité avec laquelle les entreprises et les individus sont forcés de composer. Et comme chacun fourbit ses armes de son côté, les stratégies d'attaques se perfectionnent en même temps que les techniques de protection se raffinent. Ce qui est clair, c'est que plus personne ne peut se permettre d'ignorer le phénomène.

Pour les entreprises, la lutte anti-spam n'est plus une option. Elle devrait normalement faire partie de toute politique de sécurité et être intégrée dans l'architecture de messagerie de l'entreprise. De nos jours, pour toutes les entreprises, et à plus forte raison pour les grandes sociétés et les organismes gouvernementaux, l'architecture de messagerie doit concilier plusieurs exigences : conformité réglementaire, archivage des courriels et filtrage à la sortie.

Heureusement, depuis quelques années, d'excellentes techniques de lutte au pourriel s'offrent aux gestionnaires. Utilisées conjointement, ces techniques permettent d'atteindre des taux d'efficacité de plus en plus élevés et tout à fait satisfaisants. Avec la bonne sélection, on peut maintenant atteindre près de 100 % d'efficacité et ce, avec un très faible taux de faux positifs.

En outre, les solutions de lutte au pourriel peuvent être rentabilisées très rapidement grâce aux économies qu'elles permettent et aux avantages qu'elles procurent.

Dans les années qui viennent, il faudra s'attendre à ce que les services et fonctions logicielles basés sur la réputation des envoyeurs connaissent une expansion considérable. Les informations sur la réputation des envoyeurs obtenues au niveau du contenu seront de plus en plus analysées et réutilisées afin de fournir une protection au niveau du réseau contre les connexions indésirables.

Les technologies d'authentification, comme DKIM et SPF, sont aussi appelées à se développer davantage pour corriger l'un des problèmes fondamentaux des communications par courriel : l'absence d'identité fiable dans les échanges SMTP. Et qui dit absence d'identité dit aussi absence de sécurité.

En attendant, les gestionnaires de l'informatique ont le devoir de suivre de près l'évolution des technologies de lutte au pourriel afin de pouvoir choisir les solutions les mieux adaptées aux besoins et aux vulnérabilités de leur entreprise.

ANNEXE 1 – Exemple de session SMTP

