VADERETRO
E-MAIL SECURITY

LIVRE BLANC

De l'attaque massive à l'attaque chirurgicale,

Comment se protéger contre les e-mails suspicieux ?

Spear-phishing – Usurpation d'identité - …

Auteur
Vade Retro Technology

Octobre 2011

Sommaire

Observations

«Les beaux jours» du spam de masse sont derrière nous ! En effet, aujourd'hui grâce au fort taux d'équipement du marché en solutions de protection de messagerie toujours plus performantes et efficaces, les cybercriminels ont les plus grandes difficultés à mettre en oeuvre des attaques de spam massives et se tournent désormais vers d'autres formes d'attaques plus ciblées mais tout autant lucratives.

Nous connaissons aujourd'hui le spam, le scam, le phishing pour lesquels de nombreuses techniques existent et permettent de bloquer ce type d'attaque avec une grande efficacité (réputation, signature heuristique, etc). Actuellement utilisées dans un contexte de blocage automatique sur le Mail Transfer Agent (MTA), l'ensemble de ces techniques rencontrent de plus en plus de difficultés face à la légitimité toujours plus grande du contenu des messages.

En effet, pour passer au travers des filtres antispam les plus sophistiqués, les cybercriminels s'orientent vers des attaques dites "chirurgicales". Ils étudient au préalable l'identité du destinataire et de ses proches sur les réseaux sociaux afin de créer un e-mail reproduisant le contexte interpersonnel allant même jusqu'à usurper un expéditeur connu du destinataire pour effectuer des actions frauduleuses.

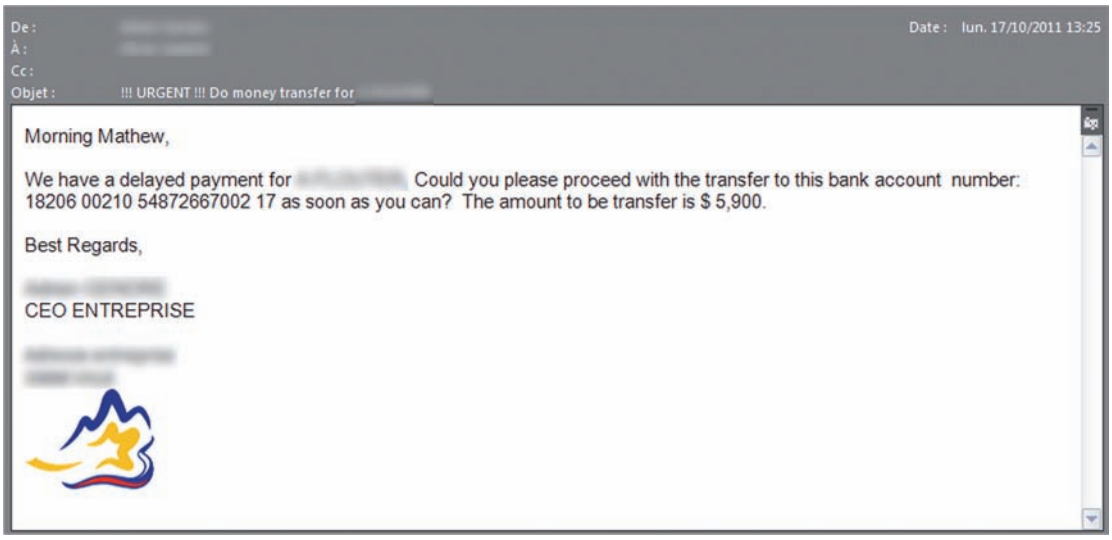
Cette usurpation d'identité est une des plus grandes menaces actuelles ? A vérifier. L'abus de confiance du destinataire basé sur des éléments réels de l'expéditeur est très difficile à déceler. Les récentes attaques d'usurpation (Intel's CEO, - Service comptabilité, Scor – Service comptabilité) démontrent à quel point cette "nouvelle menace 2.0" est à prendre au sérieux.

Le procédé rencontré jusqu'à présent est rigoureusement le même :

- L'adresse d'un haut dirigeant est usurpée afin d'envoyer un e-mail à destinatation du service de financier de l'entreprise
- Le mail demande d'effectuer un virement à un destinataire d'un compte en particulier.
- Pour plus de crédibilité, une fausse facture en retard de paiement ou autre document peut être jointe.
- De plus, afin que l'attaque soit la plus discrète possible, le contenu du mail indique de procéder à cette opération avec la plus grande discrétion. Les sommes engagées sont conséquentes (798 200 € pour Scor)

Le schéma 1 présenté ci-dessous montre un exemple d'e-mail perçu comme suspicieux mais crédible par le destinataire :

Schéma 1- Exemple d'e-mail suspicieux



Cet e-mail est un échange vu comme légitime que ce soit par un humain ou par un moteur classique d'analyse antispam. Ce type de demande peut donc avoir un impact non négligeable la réputation sur le bilan comptable de l'entreprise victime.

Comment détecter et gérer ce type d'e-mail ?

Les techniques courantes d'analyse contre les menaces transmises par e-mail ne sont pas assez efficaces face à ce type de menace grandissante. L'e-mail est trop ciblé, en faible volume voire à usage unique et trop proche d'un mail interpersonnel pour être détecté de façon automatique.

Pour pallier à ce problème, certaines entreprises définissent des règles spécifiques sur leur solution antispam ou relais de messagerie comme l'interdiction de réceptionner les e-mails provenant de l'extérieur du réseau utilisant le même nom de domaine. En plus des contraintes d'utilisation engendrées par cette technique, elle ne résout que partiellement le problème car de nombreuses parades existent

- Utilisation de noms de domaines quasi-identiques pour tromper l'oeil humain,
- Utilisation des adresses personnelles ou autres alias,
- Intrusions, machines vérolées,
- etc.

Des techniques très poussées existent pour détecter ce type d'e-mail :

- Recherche de mots clefs ou utilisation du bayésien,
- Analyse heuristique,
- Analyse sémantique.

Ces techniques identifieront ce type d'e-mails ainsi que tous les e-mails légitimes contenant des transferts de fond, ou l'envoi des mots de passe par exemple. L'automate doit donc être très vigilant sur l'action à effectuer. Une action trop brutale comme le DROP ou la mise en quarantaine créerait un nombre trop important de faux positifs et entravera la productivité d'une entreprise.

La réponse de Vade Retro Technology

Pour répondre à cette problématique, Vade Retro Technology a mis au point un nouveau module de filtrage qui peut être associé avec n'importe quelle solution de protection de messagerie déjà en place.

Le module «E-mails Suspicieux» permet de détecter ce type d'e-mail grâce à l'expérience et la précision du moteur Predictive Heuristic Filter. Vade Retro a développé une série de règles heuristiques rassemblant plusieurs techniques d'analyse et permettant de différencier ce type d'e-mail par rapport à du spam, virus ou toute autre menace. Cette précision permettra d'attribuer à ce type de menace une action spécifique.

L'action conseillée par Vade Retro Technology est la dépose du message en boite de réception mails en y intégrant le TAG de son choix (Ex : «DONNEES SENSIBLES :»). Cette alerte permettra à l'utilisateur de valider le contenu de l'e-mail ainsi que son expéditeur.

A propos de

Vade Retro Technology

Avec la protection de plusieurs centaines de millions de boîtes aux lettres dans le monde, Vade Retro Technology est le spécialiste de la messagerie contre tous les types de courriers indésirables. Outre la protection des plus grands fournisseurs d'accès Internet français et internationaux, l'entreprise protège également des milliers de PME et grandes entreprises ainsi que plusieurs millions d'indépendants et particuliers.

40C2V3-05/12 FR