Découvrez les techniques de persuasion utilisées par les cybercriminels

3

	**Découvrez les techniques de persuasion utilisées par les cybercriminels**

L**e rapport « Piratage de l'OS humain » d'Intel Security réalisé avec Europol révèle les techniques de persuasion utilisées par les cybercriminels ainsi que les méthodes de manipulations des hackers pour rendre les collaborateurs d'entreprises complices/acteurs d'actes de cybercriminalité.**

A titre de repère, les deux tiers des emails dans le monde sont des spams qui visent à extorquer des informations personnelles et confidentielles ainsi que de l'argent. Avec un coût global de la cybercriminalité estimé à 392 milliards d'euros par an, Intel Security encourage les entreprises à éduquer leurs collaborateurs face aux six leviers d'influence utilisés par les hackers. Une démarche soutenue par Europol pour limiter l'influence des hackers en europe de l'ouest

Publié quelques jours après la révélation d'une cyberattaque qui a touché plus de 100 banques à travers le monde et causé aux alentours de 900 millions d'euros de dégâts, ce rapport démontre toute l'importance d'une prise de conscience collective et souligne la nécessité d'éduquer les collaborateurs aux méthodes de persuasion appliqués par les hackers dans le monde numérique. Dans l'exemple cité, les attaques de phishing ciblées ont permis l'ouverture de brèches au sein de ces réseaux bancaires, démontrant ainsi la faiblesse intrinsèque du « pare-feu humain ». A titre de comparaison, l'étude Threat Report d'Intel Security a permis, en septembre dernier, de révéler que 92 % des employés français n'étaient pas en mesure d'identifier un courriel de phishing sur sept.

« L'analyse de nombreux cas d'usurpation de données nous montre qu'aujourd'hui, le facteur humain est le plus souvent la clé qui permet aux hackers d'agir. En les manipulant, ils les incitent à prendre des mesures qui facilitent l'infection des systèmes par des logiciels malveillants », commente Raj Samani, Directeur Technique EMEA d'Intel Security (photo)et conseiller auprès du Centre européen de lutte contre la cybercriminalité d'Europol.

« Aujourd'hui, les cybercriminels n'ont pas nécessairement besoin de savoir-faire technique pour atteindre leurs objectifs. Certains logiciels malveillants peuvent infecter les ordinateurs en y accédant directement par emails. Ces attaques ciblées manipulent les victimes et les incitent à ouvrir des pièces jointes, prétendument légitimes, ou à cliquer sur un lien qui semble provenir d'une source sûre », indique Paul Gillen, directeur des opérations du Centre Européen de lutte contre la cybercriminalité.

Sur l'année 2014, McAfee Labs a répertorié une augmentation spectaculaire du nombre d'URL malveillantes soit plus de 30 millions de liens suspects. Cette augmentation peut être attribuée à la fois à une forte hausse du nombre de liens de phishing ainsi qu'à une utilisation plus commune des URL courts qui cachent, souvent, des sites Web malveillants. Cette tendance est d'autant plus inquiétante que 18 % des utilisateurs visés par un email de phishing cliquent sur ce lien malveillant et deviennent ainsi victimes de la cybercriminalité.

Le rapport des 500 chercheurs du McAfee Labs pointe du doigt le fait que deux tiers des emails mondiaux sont des spams qui visent à soutirer des informations et de l'argent à leurs destinataires. Face à ce constat, il est d'autant plus important que les consommateurs et les collaborateurs d'entreprises soient informés des techniques de phishing et d'escroquerie couramment utilisées dans le monde numérique.

« Aujourd'hui, les cybercriminels sont devenus de très bons psychologues, capables de jouer sur le subconscient des employés en s'appuyant notamment sur un grand nombre de tactiques de « vente » souvent utilisées dans la vie quotidienne. Pour garder une longueur d'avance sur les cybercriminels et réduire le risque d'être l'une des victimes de la cybercriminalité, les entreprises doivent non seulement optimiser leurs processus et compter sur la technologie mais aussi former leurs personnels pour pallier à la brèche dans ce qu'on nomme 'l'OS humain' », conclut Raj Samani.

Il n'a jamais été plus important de former les individus à la sécurité et à la politique de leur entreprise en matière de protection des données. Paradoxalement, une étude récente publiée par Enterprise Management Associates1 a révélé que seulement 56 % des employés avaient suivi une formation à la politique de sécurité de l'entreprise. Pour mieux protéger les informations sensibles des consommateurs et des entreprises, le rapport « Piratage de l'OS humain » d'Intel Security détaille les techniques de persuasion le plus souvent utilisées par les cybercriminels :

Restez vigilent aux six leviers d'influence des cybercriminels dans le monde numérique :

Réciprocité des échanges : Les gens ont tendance à se sentir obligés de répondre une fois qu'ils reçoivent quelque chose.

Rareté de l'offre : Les individus sont motivés par l'obtention de ce qu'ils croient être une ressource rare ou une offre limitée dans le temps et peuvent ainsi s'exposer plus facilement au cybercrime. Par exemple, un faux courriel envoyé par une banque demandant à l'utilisateur d'accepter une demande suspecte afin d'éviter la désactivation de son compte dans les 24 heures peut avoir tendance à inciter au clic.

Cohérence des engagements : Une fois engagée dans une démarche, la victime choisit très souvent de tenir ses promesses pour rester cohérente et éviter de paraître peu voire non fiable. Par exemple, un pirate peut se présenter en tant qu'un membre de l'équipe SI de l'entreprise et, après avoir fait en sorte qu'un employé s'engager à respecter tous les processus de sécurité, lui demander d'effectuer une tâche suspecte sur son poste, qui semblerait être conforme aux exigences de sécurité.

Appréciation et amitié : Les tentatives d'hameçonnage sont plus productives lorsque le cybercriminel réussit à gagner la confiance de la victime. Pour endormir la méfiance, un pirate pourrait notamment essayer d'entrer en contact, soit par téléphone soit en ligne, et « charmer » au préalable sa victime potentielle.

Respect de l'autorité : Les gens ont tendance à se conformer à une figure d'autorité. Les directives dans un email prétendument envoyé de la part d'un PDG de l'entreprise sont plus susceptibles d'être suivies par un employé.

L'effet de masse : Les gens ont tendance à se conformer à la majorité. Par exemple, si un courriel de phishing est prétendument envoyé à un groupe de collègues, plutôt qu'à un seul destinataire, la victime potentielle de l'attaque se sent davantage rassurée et est plus susceptible de croire que l'email provient d'une source sûre.

Lire le rapport d'Intel Security : http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.informatiquenews.fr/les-techniques-de-persuasion-utilisees-par-les-cybercriminels-intel-security-30570
Par Enterprise Management Associates

cybercriminalité