Comment un pirate a fait pour pirater Le FBI ?

Comment un pirate a fait pour pirater Le FBI ?

Il y a quelques jours un pirate a pris contact avec le site Motherboard pour se vanter d'avoir récupéré des données sur un ordinateur du département de la Justice américain. Aujourd'hui un autre site, The Telegraph, indique que, selon un porte-parole du service, les données ne seraient pas à caractère sensible mais que des investigations sont en cours.
Sur le site qui a dévoilé l'affaire en premier il est intéressant de suivre le récit de l'attaquant qui a réussi à pirater le système.

Tout a commencé lorsqu'il a réussi à avoir accès à un compte email appartenant à sa victime, un employé du département de la justice. Il n'explique pas comment il a pu obtenir cet accès mais a pu utiliser le compte puisqu'il est rentré en contact avec le journaliste par ce biais.

Le département de la justice a fourni le code
A partir du compte le hacker a tenté de se connecter, sans succès dans un premier temps, au portail intranet du département de la Justice. Devant cet échec, il a ensuite directement pris contact avec le support du service prétextant être nouveau et n'arrivant pas à accéder au portail. Son correspondant l'a simplement questionné pour savoir s'il était en possession du code de sécurité et, constatant que ce n'était pas le cas, lui en a fourni un sans difficulté.

Une fois connecté au service, le pirate a ensuite pu prendre la main à distance sur l'ordinateur personnel de sa victime. C'est ce qui lui a permis de récupérer les données, dont les noms et informations de contacts de 22000 employés du FBI. Sur 1 To de fichiers, seuls 200 Go seraient passés entre les mains du pirate qui dit détenir des documents incluant des informations de contact de militaires et des numéros de cartes de crédit.
Un compte email est relativement simple à pirater puisqu'il s'agit la plupart du temps de deviner ou dérober le mot de passe grâce à des méthodes d'ingénierie sociale. Des protections supplémentaires existent pourtant, la plupart des services proposent notamment un système de double authentification qui nécessite la saisie d'un code reçu par SMS en plus du mot de passe… [Lire la suite]

Réagissez à cet article

Source : *Piratage du FBI : le hacker a simplement demandé le code d'autorisation – CNET France*

Attaque par phishing simulée au PMU : 120 employés piégés | Le Net Expert Informatique

	Attaque par phishing simulée au PMU : 120 employés piégés

La pièce jointe que l'on ouvre et qui diffuse un virus dans toute l'entreprise demeure le vecteur principal des attaques informatiques. Le PMU a testé les réactions de ses collaborateurs en mai dernier en leur envoyant un email de ce type conçu par ses soins. 22% ont cliqué dans la pièce jointe.

Le hack, c'est trop facile. Environ 120 collaborateurs du PMU se sont laissés piéger par un faux email leur proposant de gagner un iPad. Ils ont cliqué dans le lien présent dans l'email et donné leurs coordonnées.

6% ont donné leurs coordonnées

C'est le résultat d'un test mené en vraie grandeur par le PMU en mai dernier pour mesurer la résistance à une attaque par phishing de ses collaborateurs. Résultat : 22% des salariés ont ouvert la pièce jointe associée à un faux email d'invitation à participer à un jeu pour gagner un iPad.

Et 6% – soit environ 120 personnes – ont cliqué sur le lien présent à l'intérieur et donné leurs coordonnées pour gagner le lot. La pièce jointe affichait un faux message destiné à effrayer durant quelques minutes ceux qui l'avaient ouverte en leur faisant croire que leur PC est en danger et va être vidé.

Le test a été réalisé de façon anonyme, par un prestataire externe, en revanche, on sait que ce sont des personnes de tous les services qui ont cliqué dans l'email.

L'attaque contre TV5 monde

La DRH a donné le feu vert à l'opération car le test a été réalisé juste après les incidents de TV5 Monde qui avait vu la chaîne être bloquée durant une journée à la suite d'une attaque informatique.

Le résultat est à la fois inquiétant et rassurant. Inquiétant car test est intervenu après que le PMU ait procédé à deux ou trois campagnes de sensibilisation au phishing, en expliquant aux collaborateurs qu'il ne faut pas cliquer sur les liens présents dans les emailings. Rassurant, car le fait que le PMU communique de tels résultats permet de sensibiliser l'ensemble des entreprises à ce type de risques.

Le phishing est banal

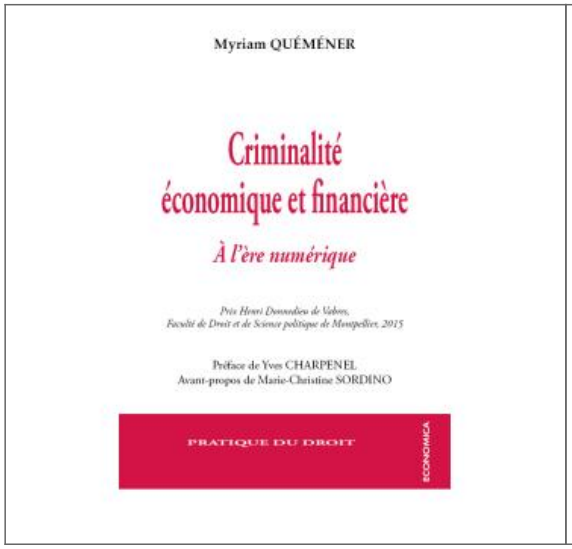
Le phishing est une attaque informatique qui consiste à envoyer des emails imitant ceux de sociétés reconnues – banques, organismes sociaux – afin de recueillir les coordonnées bancaires des personnes ciblées.

Les attaques qui propagent des virus informatiques dans les entreprises – appelées APT (Advanced Persistent Threat) – passent majoritairement par l'ouverture de pièces jointes qui diffusent ensuite un code informatique malveillant entre les machines du réseau de l'entreprise.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.larevuedudigital.com/2015/10/03/simulation-dune-attaque-par-phishing-120-employes-du-pmu-pieges/

La criminalité économique et financière à l’ère numérique | Le Net Expert Informatique



La criminalité économique et financière à l’ère numérique

Les banques, les compagnies d'assurances, les sites gouvernementaux, les compagnies pétrolières et, maintenant, l'industrie aéronautique avec la cyberattaque de la compagnie polonaise LOT : le cybercrime cible des secteurs de plus en plus sensibles, sources de dégâts humains majeurs. Au-delà des pertes financières, c'est le cœur du système politique, économique et juridique qui est aujourd'hui menacé par ce fléau.

Que fait l'État, la justice, pour enrayer ces comportements ? Fabriquer des lois en série est-elle « la » solution face à l'existence de cyberparadis, d'une cyberéconomie souterraine de plus en plus puissante, et à la volatilité des preuves ? Le Point.fr a interrogé Myriam Quemener, magistrate, auteur d'un ouvrage de référence sur le sujet : La criminalité économique et financière à l'ère numérique*.

Le Point.fr : « Certaines formes de cybercriminalité sont le fait de réseaux mafieux structurés issus de pays n'ayant pas de législation dédiée à ce phénomène », écrivez-vous. Le décalage entre les législations étatiques est-il surmontable et à quelle échéance ? Que font les autorités françaises en attendant une prise en charge globale et harmonisée de cette délinquance ?
Myriam Quemener : Les pays européens ont harmonisé leurs législations et la coopération internationale se renforce en permanence. La Convention de Budapest, seul traité relatif à la lutte contre la cybercriminalité, a déjà été signée par 46 pays, et d'autres États sont actuellement en négociation pour y adhérer. Pour ce qui concerne la France, notre pays dispose d'un arsenal ancien, en particulier la loi de 1988 dite « loi Godfrain » qui permet de réprimer les piratages informatiques et les cybermenaces. Cet arsenal s'est progressivement enrichi et perfectionné pour permettre le recours à des procédures adaptées à l'univers numérique. De nouvelles structures sont nées, comme l'Anssi, qui met en œuvre la stratégie gouvernementale en matière de cybersécurité, mais aussi une nouvelle sous-direction de lutte contre la cybercriminalité et un pôle numérique au parquet de Paris qui a vocation à s'étoffer. On a aussi créé le procureur de la République financier à compétence nationale exclusive en matière de délits boursiers et pour les affaires économiques et financières complexes qui sont aussi souvent à dimension internationale.

Quels sont les nouveaux moyens d'investigation des enquêteurs pour déjouer les attaques ?
Sur le plan procédural, le législateur a transposé le régime des interceptions téléphoniques à Internet. Il a aussi innové en prévoyant l'infiltration numérique, qui est une enquête sous pseudonyme. Elle permet à l'enquêteur d'utiliser un nom d'emprunt pour entrer plus facilement en contact avec le cyberdélinquant. Depuis la loi du 13 novembre 2014, l'enquête sous pseudonyme jusqu'alors utilisée en matière de pédopornographie et de contrefaçon s'applique à l'ensemble des procédures de criminalité organisée.

Les données personnelles sont considérées comme « l'or noir du XXIe siècle ». La semaine dernière, une importante base de données américaine abritant les coordonnées, données de santé et autres informations personnelles d'environ 20 millions de fonctionnaires a été piratée. Quel usage les cyberdélinquants font-ils des données récupérées, et à quoi peut-on s'attendre dans les années qui viennent ?
Ils récupèrent ces données et les revendent sur les marchés noirs du Web (Darknet) qui sont des réseaux parallèles aux réseaux ouverts du type Google. Cela permet par exemple de faire des achats sous de fausses identités ou d'obtenir des virements en se faisant passer pour une entreprise connue. Les données personnelles servent aussi à créer de faux profils, et tout cela se répercute sur l'e-réputation des entreprises. L'usurpation d'adresses IP (spoofing) qui permet de commettre des fraudes à la téléphonie mobile se développe aussi de manière considérable.

Quels sont les prochains défis de la criminalité astucieuse sur Internet ?
En cette période où le terrorisme frappe de façon dramatique, il est important de s'attaquer avec vigueur au financement du terrorisme, et cette lutte passe par une politique publique pragmatique et déterminée contre des phénomènes comme le cyberblanchiment ou les escroqueries aux faux ordres de virement.
Il faut par ailleurs être attentif et vigilant face à des outils numériques comme le crowdfunding (financement participatif) ou les crédits à la consommation. Les sommes obtenues au travers de ces formes de prêt peuvent en effet servir à financer des activités illicites. Il en est de même du « trading haute fréquence » qui permet d'envoyer des ordres d'achat à une vitesse de l'ordre de la nanoseconde, grâce à des algorithmes superpuissants, permettant des manipulations de cours. Le courtage à haute fréquence a aussi ses dérives : un courtier londonien a récemment été arrêté pour une manipulation sur le marché des contrats à terme électroniques aux États-Unis, qui avait contribué au mini-krach de mai 2010 à Wall Street.
Il faut aussi suivre avec attention le développement de ces fameuses « monnaies virtuelles » qui contournent le système bancaire et permettent d'échapper à tout contrôle étatique en raison de l'absence de traçabilité. Les objets connectés, qui favorisent l'usurpation de profils complets, et le cloud computing qui contient des données sensibles à valeur commerciale sont aussi des cibles potentielles de cyberattaques. D'autant que de nombreuses failles de sécurité existent et peuvent être exploitées par les cybercriminels.

Qu'est-ce qui dissuade vraiment les délinquants, qu'ils soient isolés ou membres d'organisations criminelles ?
La mise en place d'une stratégie globale au niveau des services de l'État est de nature à dissuader les cyberdélinquants, de même que les condamnations et démantèlements de réseaux de cybercriminels qui ne cessent d'augmenter grâce aux moyens d'investigation et à l'expertise de plus en plus pointue des enquêteurs dédiés.

Pensez-vous que l'Internet a démultiplié les risques, ou les a-t-il seulement déplacés ?
L'absence de confrontation physique auteur-victime, propre à Internet, facilite le passage à l'acte. Le système des rencontres virtuelles attire des personnes mal intentionnées qui peuvent plus facilement extorquer de l'argent, notamment via des sites de vente entre particuliers. Aujourd'hui, la cybercriminalité s'industrialise et s'organise sous forme de structures hiérarchisées allant de la main-d'œuvre de base qui récupère des données jusqu'aux têtes de réseau qui donnent les ordres.

Ces phénomènes sont-ils, comme le changement climatique, irréversibles ?
Je ne le pense pas, car, actuellement, il y a une mobilisation importante, du secteur tant public que privé, pour lutter contre ces phénomènes. Il est indispensable de multiplier les actions de formation pluridisciplinaire des acteurs publics et privés qui concourent à la lutte contre ces attaques. Cependant, il ne faut pas perdre de vue que ce type de délinquance lance un défi au temps judiciaire, c'est même une course contre la montre !

L'ouvrage en vente ici

Source : http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/cybercrime-un-defi-lance-au-temps-judiciaire-13-07-2015-1943938_56.php

---

Exclusif : 47 grandes entreprises françaises ciblées par une tentative d'escroquerie à grande échelle | Le Net Expert Informatique

47 grandes entreprises françaises ciblées par une tentative d'escroquerie à grande échelle

Selon nos informations, une cinquantaine de grandes entreprises sont actuellement – ou ont été au cours des derniers jours – la cible d'un réseau criminel spécialisé dans l'escroquerie aux faux ordres de virement (FOVI), encore appelée « Arnaque au président ». La technique n'est pas nouvelle. Ce qui interpelle, dans le cas présent, c'est l'ampleur de l'offensive mise à jour.

« L'arnaque au président » n'est pas vraiment d'un genre nouveau. D'ailleurs son pionnier, Gilbert Chikli, poursuivi par 33 banques et aujourd'hui réfugié en Israël, vient d'être condamné par contumace à 7 ans de prison et à 1 millions d'euros d'amende.

En cause : des escroqueries jugées « hors-norme », dont l'essaimage est devenu en quelques mois la bête noire des grandes directions financières, à commencer par celles que l'on pensait être les plus aguerries. Ainsi en 2012, c'est KPMG qui en a fait les frais : le géant mondial de l'audit et du conseil en fiscalité a laissé s'envoler à son insu pas moins de 7,6 millions d'euros.

Ces tentatives d'escroquerie n'épargnent personne : pas plus Michelin ou le Palais de l'Elysée, que nos PME régionales. Si Gilbert Chikli promet aujourd'hui avoir tiré sa révérence, il n'est en revanche pas improbable qu'il ait, directement ou non, inspiré quelques disciples.

47 entreprises sous la menace imminente de la criminalité financière

C'est une longue liste de cibles que s'est procuré la rédaction du JDE, par l'intermédiaire d'un cabinet privé spécialisé dans l'investigation et la lutte anti-fraude. Pour des raisons évidentes de sécurité, les consultants qui nous ont transmis cette information préfèrent rester anonymes.

Ils témoignent : « la spécificité de cette affaire réside dans l'ampleur de l'attaque. A ce jour, nous ne pouvons confirmer son état de progression ou son éventuel aboutissement. Nous avons contacté chacune des entreprises ciblées pour tenter d'être mis en relation avec les directions générales ou financières afin de de les en avertir. Malheureusement, le personnel n'étant pas toujours sensibilisé à ce type de risque, certains de nos appels sont restés sans suite. »

Une situation qui n'étonne guère ces analystes rompus à la gestion des affaires réservées des dirigeants : «Malheureusement, ces escroqueries aboutissent la plupart du temps à cause de défaillances dans la sûreté et les procédures internes de l'entreprise. La formation des collaborateurs, la circulation intelligente de l'information et l'instauration de procédures de vérification restent les meilleurs remparts contre ces attaques. »

Parmi les entreprises ciblées ou déjà attaquées, recensées par les enquêteurs, on retrouve de grands noms de l'économie française, des groupes familiaux plus discrets, et des enseignes bien connues des Français. « Des attaques qui sont en préparation depuis fin avril », précisent nos interlocuteurs, qui nous livrent ci-après le nom des entreprises ou organismes concernés :

Direction Finance, Ludendo, Système U, Abbott, 3 Suisses, GE Capital, Sonepar, Joué Club, Monoprix, BHR Béton, La Redoute, Eurofactor, Sephora, Picard, Imerys, Groupe Flo, GSF, DB Apparel, Optic 2000, Marionnaud, Groupe Pigeon, Invacare, Franck Provost, Auchan, Continental Corporation, Pronatura, Finifac, Provalliance, Carrefour, Vivendi, Korian, Accor, Servair, Bricorama, SKF, SNEF, SNCF, Rexel, Ecolab, Soprasteria, Chausson Matériaux, Faurecia, Immochan, Eiffage, Clemessy.

Comment réagir en cas d'attaque ?

« Nous avons pris des mesures directes pour tenter d'endiguer la marge de manœuvre des 'assaillants' et prévenir le risque d'escroquerie, et travaillons en étroite relation avec nos partenaires depuis plus d'un mois, expliquent les analystes. Surtout, nous accompagnons nos clients dans la mise en place d'une procédure judiciaire à l'encontre des auteurs de la tentative d'escroquerie, en sachant pertinemment qu'elle sera longue et complexe. »

D'après le cabinet, en effet, les quelques traces électroniques analysées laissent apparaître un mode opératoire assez classique, probablement piloté depuis Israël ou un territoire voisin comme l'indiquent les paquets de données qui ont été analysés.

« Dans certains pays, les moyens de paiement prépayés sont très répandus et peu régulés, donc difficilement traçables. Ils peuvent être ensuite utilisés en France, pour acquérir de l'information légale sur les sociétés ou à l'étranger, pour recourir anonymement aux services d'une plateforme téléphonique ». Ce sont également ces cartes prépayées qui, en toute vraisemblance, auront permis aux escrocs de réserver des noms de domaine pour peaufiner leur déguisement électronique.

Un déguisement qui va, selon les experts, jusqu'à l'usurpation d'identité de personnes vivantes ou décédées : « Pour brouiller les pistes, ces brigands 2.0 utilisent vos adresses, numéros de téléphone, dates de naissance pour réserver des noms de domaine et procéder à certaines formalités en ligne. C'est probablement supposé divertir les enquêteurs », ironise l'un de nos experts.

Piqûre de rappel : le mode opératoire

Une opération couronnée de succès est une opération bien préparée. Les escrocs commencent par une phase de renseignement en « zone grise », en collectant un maximum d'informations sur leur cible. C'est ce qu'on appelle le « social engineering », dont le but est de recueillir suffisamment de données quant à l'environnement humain (personnes clés, numéros de téléphone, adresse email) et économique (contrats, fournisseurs, bilans, etc.) de l'entreprise.

C'est bien moins compliqué qu'il n'y paraît : munis d'une carte prépayée, il leur suffit de se rendre sur une base de données de type Infogreffe et de télécharger les documents les plus riches en information : derniers statuts et actes déposés, PV d'assemblées générales, ou comptes annuels par exemple. L'identification, sur les réseaux sociaux, des « personnes clés » dans l'organigramme de la cible permet parfois de se familiariser avec leurs futurs interlocuteurs.

Depuis une plateforme téléphonique située à l'étranger, mais avec un numéro français d'apparence, l'escroc appelle un directeur financier, un service comptable, ou tout individu ayant compétence à agir sur les comptes de l'entreprise.

Se faisant généralement passer pour le dirigeant de l'entreprise, il déploie alors des trésors de créativité et/ou de séduction. Tantôt flatteur, tantôt menaçant, il prétexte une situation d'urgence (opération boursière sensible, ou imminence d'un contrôle fiscal par exemple) et exige le virement immédiat d'une importante somme sur un compte habituellement hébergé en Chine.

Nos interlocuteurs invitent donc les entreprises à la plus grande vigilance : « ces offensives sont généralement fulgurantes et, le temps de réagir, nos escrocs sont déjà loin »…

Source : http://www.journaldeleconomie.fr/Exclusif-47-grandes-entreprises-francaises-ciblees-par-une-tentative-d-escroquerie-a-grande-echelle_a2456.html

Alerte ! Des escrocs se font passer pour des techniciens en informatique | Le Net Expert Informatique

Alerte ! Des escrocs se font passer pour des techniciens en informatique

Mercredi, une habitante de Saint-Pal-de-Mons a subi une tentative d'escroquerie par des cybercriminels. Elle a reçu un appel téléphonique d'une personne parlant anglais se présentant comme employée d'une célèbre entreprise d'informatique. Selon les dires de son interlocuteur, son ordinateur serait infecté d'un virus. L'appel a été transmis à un second présumé technicien qui, toujours en anglais, a proposé à la San-palouse de prendre la main sur la machine.

La femme a alors eu la puce à l'oreille lorsqu'on a lui a demandé ses coordonnées bancaires. Elle a raccroché et s'est rendue dans une entreprise spécialisée. Des fichiers de son ordinateur ont été endommagés.
Elle a ensuité déposée plainte auprès des gendarmes de la communauté de brigades de Saint-Didier-en-Velay.
Selon nos informations, les premiers éléments tendraient vers une escroquerie depuis l'étranger, l'indicatif « 00221 » au moment de l'appel étant celui du Sénégal.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://www.leprogres.fr/faits-divers/2015/03/13/cybercriminalite-ils-se-font-passer-pour-des-techniciens-en-informatique

La formation du personnel,

seule vraie solution contre les attaques informatiques

3

	La formation du personnel, seule vraie solution contre les attaques informatiques

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, le nouveau rapport d'Intel Security démontre toute l'importance d'une prise de conscience collective et souligne la nécessité d'éduquer les collaborateurs aux méthodes de persuasion utilisées par les hackers.

Dans ce fameux cyber-casse dont l'existence a été révélée la semaine dernière, ce sont des attaques de phishing ciblées qui ont permis de créer des brèches au sein des réseaux bancaires, démontrant ainsi la faiblesse intrinsèque du « pare-feu humain ». Ce que confirme l'étude Threat Report d'Intel Security qui indique que 92 % des employés français ne sont pas en mesure d'identifier un courriel de phishing sur sept. »Aujourd'hui, les cybercriminels n'ont pas nécessairement besoin de savoir-faire technique pour atteindre leurs objectifs, explique Paul Gillen, directeur des opérations du Centre Européen de lutte contre la cybercriminalité.
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 ».
Sur l'année 2014, McAfee Labs a constaté une augmentation spectaculaire du nombre d'URL malveillantes soit plus de 30 millions de liens suspects. Une hausse qui peut être attribuée à la fois à une forte croissance du nombre de liens de phishing, ainsi qu'à une utilisation plus commune des URL courts qui cachent, souvent, des sites Web malveillants. Le rapport des 500 chercheurs du McAfee Labs pointe par ailleurs 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.
Il est donc important que les consommateurs et les collaborateurs d'entreprises soient informés des techniques d'escroquerie couramment utilisées dans le monde numérique.
« Pour conserver 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, Directeur Technique EMEA d'Intel Security.

Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Vous souhaitez participer à une de nos formations ?
Besoin d'informations complémentaires ?
Contactez-nous

Expert Informatique et formateur spécialisé en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel, Nous sommes en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://www.infodsi.com/articles/154213/formation-personnel-seul-vrai-rempart-attaques-informatiques.html

Les 5 techniques que les cybercriminels utilisent pour pénétrer les réseaux | Le Net Expert Informatique

	Les 5 techniques que les cybercriminels utilisent pour pénétrer les réseaux

Il existe au moins 5 techniques de nature « discrète et graduelle » que les cybercriminels utilisent désormais pour pénétrer les réseaux et accomplir leur mission, et que les professionnels de la sécurité doivent comprendre et repérer afin de défendre plus efficacement leur entreprise :

1. Les kits d'exploits : les concepteurs de kits d'exploits connus comme Blackhole ont été repérés par les autorités et stoppés dans leurs actions. Les hackers ont ainsi réalisés que les attaques de grande ampleur ne sont pas toujours les plus efficaces – que ce soit de par la taille des infrastructures ou des moyens malveillants mis en œuvre. Ainsi les hackers préfèrent disposer du 4ème ou 5ème kit d'exploits le plus connu et utilisé, pour ne pas trop attirer l'attention.

2. Le spam « Snowshoe » : avec cette technique, le hacker diffuse beaucoup de messages sur une grande surface d'attaque pour échapper aux outils de détection traditionnels. Le spammeur Snowshoe envoie un email non sollicité en utilisant un grand nombre d'adresses IP mais à un faible volume de messages par adresse IP, avec pour objectif de contourner les technologies de réputation anti-spam basées sur l'adresse IP. Il change rapidement le corps du texte, les liens, les adresses IP utilisées pour la diffusion et ne répète jamais la même combinaison.

3. Le spear phishing sophistiqué : les hackers continuent d'affiner leurs messages, bien souvent en utilisant des techniques d'ingénierie sociale, de sorte que même les internautes expérimentés ont du mal à repérer les faux messages. Les récentes attaques de spear phishing semblent provenir de fournisseurs ou d'opérateurs connus, desquels les utilisateurs reçoivent régulièrement des messages – par exemple, les prestataires de services, les sites de vente en ligne et les fournisseurs de contenus musicaux et de loisirs. Ces emails peuvent contenir un nom de confiance, un logo connu et inviter le destinataire à réaliser une action familière, comme donner son avis à propos d'une commande récente, ou donner un numéro pour le suivi de sa livraison. Cette mécanique bien huilée et discrète donne aux utilisateurs un faux sentiment de sécurité, les incitant à cliquer sur des liens malveillants contenus dans l'e-mail.

4. Le partage d'exploits entre deux fichiers différents : les malwares Flash peuvent désormais interagir avec JavaScript pour cacher des activités malveillantes en partageant un exploit entre deux fichiers et formats différents : un fichier Flash, un fichier JavaScript. Cela dissimule l'activité malveillante et rend l'identification, le blocage ainsi que l'analyse de l'exploit beaucoup plus difficile. Cette approche permet également aux hackers d'être plus efficaces dans leurs attaques. Par exemple, si la première étape d'une attaque est entièrement en JavaScript, la seconde étape, le transfert du code malicieux, ne se produirait qu'après l'exécution avec succès du code JavaScript. De cette façon, seuls les utilisateurs qui peuvent exécuter le fichier malveillant reçoivent celui-ci.

5. Le malvertising : les créateurs de malwares ont mis au point un nouveau business modèle perfectionné qui utilise les modules publicitaires des navigateurs Web pour diffuser des logiciels malveillants et des applications indésirables. Les utilisateurs achètent, téléchargent et installent des outils tels que Adobe ou des logiciels vidéo depuis des sources qu'ils estiment légitimes. En réalité, ces applications sont livrées avec un logiciel malveillant. Cette nouvelle approche de diffusion de malwares est un succès pour les hackers car de nombreux utilisateurs font naturellement confiance aux publicités ou les considèrent comme bénignes. Les hackers gagnent de l'argent à partir d'un grand nombre utilisateurs, par petites touches, en infectant de manière persistante leur navigateur et en se cachant sur leur machine.

Les professionnels de la sécurité et les cybercriminels sont dans une course permanente pour tenter de déjouer l'autre. Les hackers sont de plus en plus professionnels, non seulement dans leurs approches pour lancer des attaques, mais aussi pour échapper aux outils de détection, par des moyens que nous n'avions pas vus jusqu'à présent. Mais en continuant à innover et à apprendre sur la base de ce qu'ils observent, les professionnels de la sécurité peuvent identifier et contrer ces nouvelles techniques d'attaques.

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

Source : http://www.informatiquenews.fr/quelles-reponses-aux-nouvelles-cyberattaques-christophe-jolly-cisco-31360
Par Christophe Jolly, Directeur Sécurité de Cisco France

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.

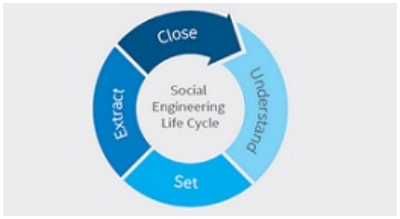
L'effet de masse : Les gens ont tendance à se conformer à la majorité. Par exemple, si un courriel de phishing est prétendument envoyé à un groupe de collègues, plutôt qu'à un seul destinataire, la victime potentielle de l'attaque se sent davantage rassurée et est plus susceptible de croire que l'email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

Les cybercriminels à la pointe de la psychologie | Le Net Expert Informatique



Les cybercriminels à la pointe de la psychologie

Les méthodes de substitution des données évoluent et se calquent de plus en plus sur des modèles de manipulation existant dans le monde réel tels que les techniques de ventes ou d'escroquerie. Nommé « piratage de l'OS humain », cette dernière publication soutenue par le Centre Européen de lutte contre la cybercriminalité d'Europol met en avant 6 leviers d'influence que les hackers utilisent pour rendre complices/acteurs les employés d'une société.

Ainsi, on parle de réciprocité des échanges pour décrire la tendance naturelle que l'homme a de répondre systématiquement aux courriels. Technique couramment utilisée dans le phishing, la rareté de l'offre motive les individus à obtenir une ressource qu'ils pensent être unique ou limitée dans le temps. Autre phénomène purement humain, la cohérence des engagements permet aux hackers de profiter de la victime qui souhaite simplement tenir ses promesses, par exemple, en suivant les processus de sécurité édictés par un pirate se présentant comme membre de l'équipe SI.
L'appréciation et l'amitié sont un facteur qui permet aux hackers d'augmenter la réussite de leur hameçonnage en gagnant la confiance d'une victime, la « charmer », en essayant notamment de rentrer directement en contact soit par le téléphone ou en ligne. Le respect de l'autorité est un autre levier. Par le biais d'un mail, le cybercriminel abuse de sa victime en se faisant passer pour le PDG de l'entreprise. Dernier levier discerné par Intel Security, un employé sous l'effet de masse a tendance à octroyer plus facilement sa confiance. Ainsi un mail malveillant aura plus d'impact s'il est envoyé à un groupe de collègues plutôt qu'à un seul destinataire.
Pour l'année 2014, McAfee Labs dénombre plus de 30 millions de liens suspects en relation avec l'augmentation des mails de phishing. Autre chiffre mis en avant dans ce rapport, 92% des employés contre 80% dans le monde se seraient déjà fait piéger par des menaces informatiques et le coût de cette cybercriminalité est estimé au total à 392 milliards d'euros par an. 2/3 des e-mails sont des spams et 18% des utilisateurs visés par mail de phishing cliquent sur ces liens malveillants, Intel Security rappelle l'importance que les entreprises doivent accorder à l'éducation de leurs collaborateurs concernant ces techniques de persuasion et d'escroquerie.

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

Source : http://www.itpro.fr/n/cybercriminels-pointe-psychologie-21105/
Par Tristan Karache

92% des salariés français sont incapables de détecter du phishing

92% des salariés français sont incapables de détecter du phishing

Le facteur humain est toujours le point faible en matière de cybersécurité. Il s'avère que 92% des salariés français sont incapables de détecter les tentatives de phishing les plus courantes. Intel Security estime que le coût global de la cybercriminalité dans le monde peut être estimé à quelque 445 milliards de dollars. Il est par ailleurs estimé que deux tiers des courriels envoyés dans le monde sont des spams destinés à extorquer de l'information ou de l'argent.

Une étude conjointe menée par McAfee Labs, filiale d'Intel Security, et le centre de cybercriminalité européen d'Europol (EC3) révèle toute l'importance du facteur psychologique dans la réussite des attaques informatiques. « **Le facteur humain est toujours le point faible en matière de cybersécurité** », a expliqué Raj Samani, le directeur technique d'Intel Security.

« Les entreprises de tous les secteurs industriels, toutes les tailles et toutes les régions du monde sont en danger en raison du facteur social », résume Raj Samani. Il explique qu'« il est important de comprendre que les cybercriminels s'avèrent souvent être de bons psychologues et que le facteur humain est souvent utilisé comme un point d'entrée pour les cyberattaques » en précisant que les hackers savent parfaitement user de la séduction, du respect de l'autorité, du conformisme social et du besoin de retourner une faveur, sans oublier la loyauté ou la peur de rater une opportunité.

Cette étude révèle par exemple qu'en France, 92% des salariés sont incapables de détecter les tentatives de phishing les plus courantes et les plus fréquemment utilisées.

Ce résultat est d'autant plus inquiétant pour les entreprises françaises que le rapport révèle que 18% des utilisateurs visés par un courriel d'hameçonnage deviennent finalement des victimes après avoir cliqué sur un lien frauduleux.

C'est ainsi que Raj Samani conclut en déclarant qu'«il est crucial pour les entreprises d'éduquer leurs employés sur la cybersécurité en plus des mesures prises sur les niveaux opérationnels et techniques».

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

Source : http://www.linformatique.org/cybercriminalite-92-des-salaries-francais-sont-incapables-de-detecter-du-phishing/
Par Emilie Dubois