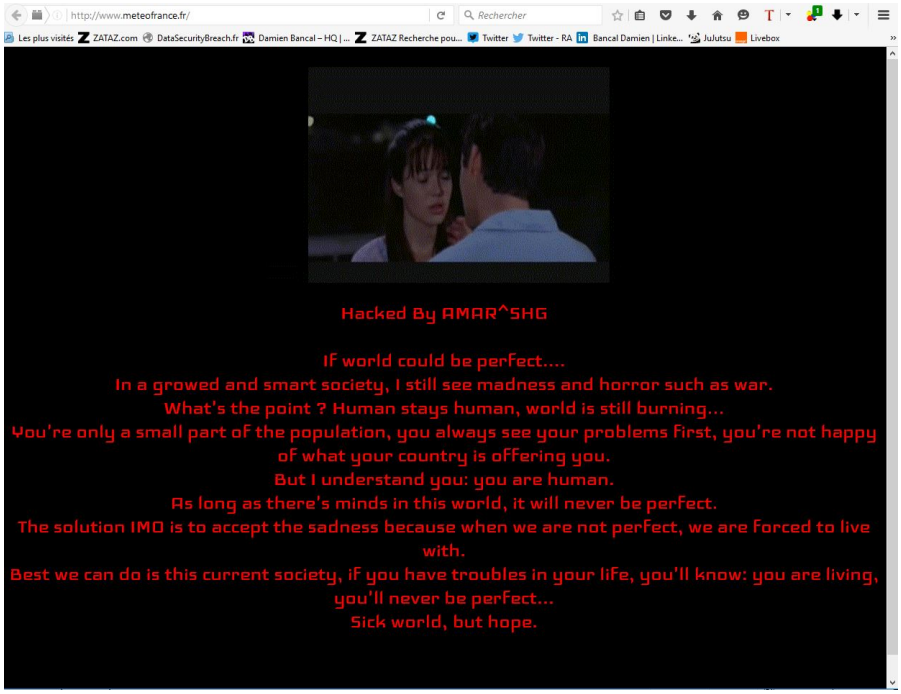
Le site Internet de Météo France piraté

	**Le site Internet de Météo France piraté**

Après les sites de Canal +, un nouveau message d'espoir mis en ligne par un pirate informatique sur l'ensemble des sites Internet de Météo France. Un détournement de DNS radical.



Il se nomme Amar^SHG. Ce jeune pirate informatique (Il serait un Albanais) est dans la mouvance des hacktivistes politiques qui, par le biais de la modification de site Internet (defacement, barbouillage), trouvent un moyen de faire passer des messages. Amar^SHG a fait la pluie et le beau temps sur les sites de Météo France via un détournement de DNS radical.
Lundi soir, le pirate a mis la main sur un moyen informatique qui lui a donné l'occasion de détourner l'ensemble des noms de domaines de Météo France. Comme il a pu me l'indiquer sur Twitter, les domaines .fr, .mobi, . Paris, … ont été impactés.

Détournement de DNS

*Les visiteurs accédaient, ce lundi soir (vers 22h30), à une page noire et rouge, portée par la musique « Wonderful life » de Katie Melua. Côté message, le cyber manifestant souhaitait viser ceux qui « **se plaignent pour leurs propres problèmes** ». AMAR ^ SHG parle d'espoir, d'un monde qui n'est pas parfait « **Il faut vivre avec, avec espoir** »… [Lire la suite]*

Article de Damien BANCAL

Réagissez à cet article

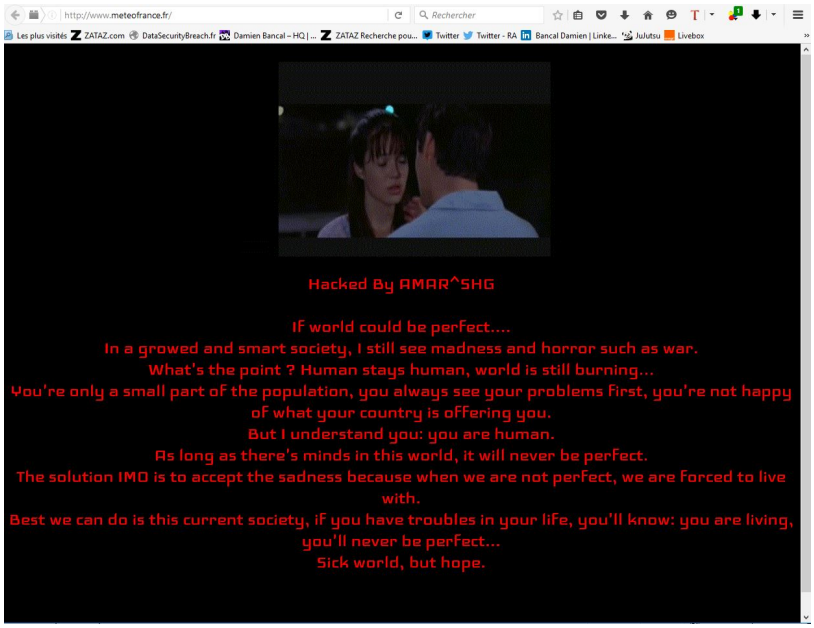
Source : *ZATAZ Détournement de DNS – Un pirate passe par Météo France – ZATAZ*

Le site Internet de Météo France victime de détournement de DNS après celui de Canal +

M

Le site Internet de Météo France victime de détournement de DNS après celui de Canal +

Après les sites de Canal +, un nouveau message d'espoir mis en ligne par un pirate informatique sur l'ensemble des sites Internet de Météo France. Un détournement de DNS radical.



Il se nomme Amar^SHG. Ce jeune pirate informatique (Il serait un Albanais) est dans la mouvance des hacktivistes politiques qui, par le biais de la modification de site Internet (defacement, barbouillage), trouvent un moyen de faire passer des messages. Amar^SHG a fait la pluie et le beau temps sur les sites de Météo France via un détournement de DNS radical.
Lundi soir, le pirate a mis la main sur un moyen informatique qui lui a donné l'occasion de détourner l'ensemble des noms de domaines de Météo France. Comme il a pu me l'indiquer sur Twitter, les domaines .fr, .mobi, . Paris, … ont été impactés.

Détournement de DNS

Les visiteurs accédaient, ce lundi soir (vers 22h30), à une page noire et rouge, portée par la musique « Wonderful life » de Katie Melua. Côté message, le cyber manifestant souhaitait viser ceux qui « se plaignent pour leurs propres problèmes ». AMAR ^ SHG parle d'espoir, d'un monde qui n'est pas parfait « Il faut vivre avec, avec espoir ».
Un message qui change des propos de haines, guerriers… que l'on peut croiser sur des pages modifiées par d'autres pirates informatiques. Une attaque qui a pu être mise en place via un phishing, un accès non autorisés à partir d'une injection SQL… Bref, plusieurs méthodes possibles ont pu être exploitées pour atteindre l'administration des noms de domaine et orchestrer ce détournement de DNS… [Lire la suite]

Réagissez à cet article

Source : *ZATAZ Détournement de DNS – Un pirate passe par Météo France – ZATAZ*

Cybercriminalité, comment l'entreprise peut se protéger ?

Cybercriminalité, comment l'entreprise peut se protéger ?

Denis Jacopini, spécialiste en cybercriminaltié et dans la protection des données personnelles interviewé par l'Entreprise connectée.

 **Il acte des formations auprès des dirigeants d'entreprises et des salariés, pour leur donner des conseils et détecter les attaques. Il nous donne son avis d'expert pour aider les entreprises dans la prévention des cyberattaques.**

EC: Quels sont les risques de la cybercriminalité ?
Denis Jacopini : La cybercriminalité prend plusieurs formes : des pirates qui ont message à faire passer et dont le but est la défiguration de sites internet, et d'autres qui recherchent l'aspect pécuniaire de la cybercriminalité. Une attaque entraine une mauvaise image et une perte de confiance autant auprès des clients que des salariés. Ces derniers risquent de moins s'engager dans l'entreprise et de perdre confiance dans la sécurité informatique avec la peur de voir leurs données personnelles volées.
EC: Que conseillerez-vous aux entreprises pour améliorer leur sécurité ?
DJ : Les entreprises ont conscience de la cybercriminalité mais se font toujours avoir. Il faut absolument éduquer. Toutes les entreprises risquent de se faire pirater. L'élément souvent négligé est la charte informatique qui va lier le salarié aux usages des outils informatiques.
EC: Et concrètement ?
DJ : Concrètement, pour anticiper, l'entreprise doit, faire un audit de la sécurité de son système d'information (analyses des mesures de sécurité existantes, test d'intrusion, analyse des usages illicites internes ou externes à l'entreprise) et prévoir une sensibilisation des salariés par un organisme extérieur. Les actions qui en ressortent souvent sont : l'amélioration d'outils et de mesures de sécurité, la mise en place d'une charte informatique, d'outils de cryptage des e-mails ou de cryptage des données. Enfin, la mise à niveau tous les 12 mois des employés car ils doivent connaître les nouvelles techniques couramment utilisées par les cybercriminels.
EC: Quel est le plus grand danger pour les entreprises ?
DJ : La plus grande menace reste le mail piégé. Dans la précipitation, l'employé va l'ouvrir et cliquer sur une page web usurpée. A partir de là, le pirate peut s'infiltrer, c'est ce qu'il s'est passé avec TV5 Monde. Contre ce genre d'attaque, appelée « spear-phising », la technologie arrive à ses limites. La question désormais, est celle du comportement. La sensibilisation des salariés est très difficile mais il est possible de leur apprendre toutes les formes d'attaques, grâce à des formations. … [Lire la suite]

Réagissez à cet article

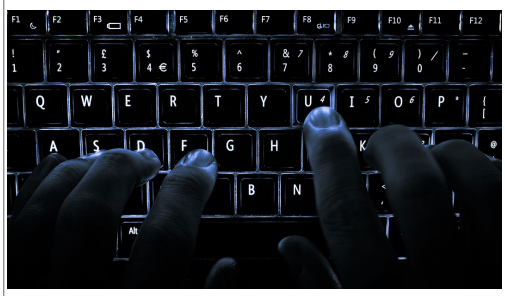
Source : *Cybercriminalité, comment se protéger ? – L'entreprise connectée*

Comment les hackers font-ils pour pirater toutes vos données informatiques ?

Comment les hackers font-ils pour pirater toutes vos données informatiques ?

Aujourd'hui, les informations sont partout avec le développement d'Internet. Il est donc important de savoir se prémunir contre les techniques employées pour nous pirater ou nous nuire. Surtout que les hackers, ces pirates du web, se développent de plus en plus et emploient des techniques toujours plus redoutables. SooCurious vous présente les techniques développées par ces génies malveillants de l'informatique.

Vous le savez certainement, le monde d'Internet est dangereux et est le terrain de jeu de personnes malveillantes. Ces gens sont appelés des hackers : ce sont des pirates informatiques qui se servent de leur ordinateur pour récupérer des informations privées ou pour infiltrer des serveurs de grosses entreprises. D'où l'importance de bien choisir ses mots de passe. Avant de pirater, le hacker va enquêter sur sa cible. Il va chercher tout ce qu'il peut savoir sur la personne, à savoir l'adresse IP, le type de logiciels installés sur l'ordinateur de la « victime ». Ils trouvent facilement ces informations grâce aux réseaux sociaux, aux forums en ligne. Une fois qu'ils ont récupéré ces données, le travail de piratage peut commencer.



Hacker n'est pas à la portée de tout le monde : il faut une maîtrise totale de l'informatique pour y parvenir. Ces pirates 2.0 ont plusieurs techniques pour parvenir à leurs fins. La première d'entre elles est le clickjacking. L'idée est de pousser l'internaute à fournir des informations confidentielles ou encore de prendre le contrôle de l'ordinateur en poussant l'internaute à cliquer sur des pages. Sous la page web se trouve un cadre invisible, comme un calque, qui pousse la personne à cliquer sur des liens cachés.
Par exemple, il existe des jeux flash où l'internaute doit cliquer sur des boutons pour marquer des points. Certains clics permettent au hacker d'activer la webcam.

Autre technique, peut-être plus courante, celle du phishing.
Appelée aussi l'hameçonnage, cette action opérée par le pirate vise à soutirer une information confidentielle comme les codes bancaires, les mots de passe ou des données plus privées. Pour récupérer un mot de passe, un hacker peut aussi lancer ce qu'on appelle « une attaque par force brute ». Il va tester une à une toutes les combinaisons possibles (cf. faire un test avec Fireforce) avec un logiciel de craquage. Si le mot de passe est trop simple, le hacker va rapidement pénétrer votre ordinateur. D'autre part, les hackers cherchent parfois à craquer les clés WEP, afin d'accéder à un réseau wi-fi. Encore une fois, si la clé est trop courte, le craquage est facile. Le hacking se développant, des techniques de plus en plus pointues se développent.

Vol des données bancaires via Shutterstock
Il existe maintenant des armées de hackers ou des groupes collaborant dans le but de faire tomber des grosses entreprises ou des banques. Début 2016, la banque internationale HSBC a été piratée. A cause de cela, leur site était totalement inaccessible, ce qui a créé la panique chez les clients de cette banque. Cet épisode n'est pas isolé. Il est même le dernier d'une longue série. Pour parvenir à semer la panique dans de grandes firmes, ils utilisent des techniques plus ou moins similaires à celles présentées ci-dessus, mais de plus grande envergure.

La technique du social engineering n'est pas une attaque directe.
C'est plutôt une méthode de persuasion permettant d'obtenir des informations auprès de personnes exerçant des postes clés. Les pirates vont cibler les failles humaines, plutôt que les failles techniques. Un exemple de social engineering serait l'appel fait à un administrateur réseau en se faisant passer pour une entreprise de sécurité afin d'obtenir des informations précieuses.

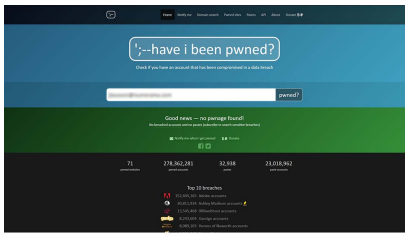
Autre méthode, celle du défaçage.
Cette dernière vise à modifier un site web en insérant du contenu non désiré par le propriétaire. Cette méthode est employée par les hackers militants qui veulent dénoncer les pratiques de certains gouvernements ou entreprises. Pour ce faire, le hacker exploite une faille de sécurité du serveur web hébergeant le site. Ensuite, il suffit de donner un maximum d'audience au détournement pour décrédibiliser la cible. En avril 2015, le site de Marine Le Pen a été victime de défaçage : des militants ont publié une photo de femme voilée avec un message dénonçant la stigmatisation des musulmanes par le FN.

Enfin, les hackers se servent aussi du DDOS (déni de service distribué), qui sature un service pour le rendre inaccessible et du Buffer Overflow, qui provoque une défaillance dans le système pour le rendre vulnérable… [Lire la suite]

Réagissez à cet article

Source : *Comment les hackers font-ils pour pirater toutes vos données informatiques ? | SooCurious*

Comment vérifier si vos données ont été piratées

	**Comment vérifier si vos données ont été piratées**

Un service sur lequel vous êtes inscrit a été piraté et vous craignez pour vos données personnelles ? Un site permet de vérifier si votre e-mail est concerné.
Il ne se passe pas une semaine sans que l'actualité ne se fasse l'écho d'une attaque informatique ayant visé un site web ou une application, et leurs données personnelles. Et l'histoire est souvent la même d'une affaire à l'autre. Il s'agit en général de pirates qui profitent d'une faille dans la protection du service pour dérober les données personnelles de ceux qui ont ouvert un compte en faisant confiance à la sécurisation des données.

Gare à votre e-mail !

Ces informations sont ensuite diffusées sur le net, exploitées pendant des actions de phishing (hameçonnage) destinées à récupérer frauduleusement d'autres éléments ou bien font l'objet d'un commerce.
Normalement, les sites qui ont fait l'objet d'un piratage alertent leurs membres par mail. En règle générale, celui-ci comporte des indications sur ce qui s'est passé et, surtout, des recommandations à suivre sans tarder : modification du mot de passe et surveillance des comptes en banque, par exemple.
Mais il peut arriver que ce courrier ne soit pas vu par le destinataire : parce qu'il est tombé dans les spams, parce qu'il a été supprimé par mégarde ou parce que l'internaute utilise depuis un moment une nouvelle adresse de courrier électronique.
EST-CE QUE JE ME SUIS FAIT AVOIR ?
*D'où l'intérêt d'un site comme « **Have I Been Pwned ?** » (que l'on pourrait traduire par « est-ce que je me suis fait avoir ? »). Le principe est simple : vous entrez votre adresse mail dans le champ prévu à cet effet et le site vous indique si votre mail est concerné par une fuite de données personnelles.*
Deux cas de figure peuvent se présenter.

Pas de problème !
Si votre mail n'est pas recensé sur « Have I Been Pwned ? », c'est bon signe. Cela veut dire que sur les services dont le site assure le suivi, votre adresse n'a – a priori – pas fait l'objet d'une fuite. Mais attention, si le site ne trouve rien, cela ne veut pas dire que tout va pour le mieux dans le meilleur des mondes.
En effet, vous êtes peut-être présent sur des services dont le piratage n'a pas été relevé par « Have I Been Pwned ? », ou dont les listings de données n'ont pas été diffusés. De plus, il peut être sage de vérifier que tout va bien avec vos autres adresses, si vous en avez. Car peut-être étiez-vous inscrit avec un ancien mail.

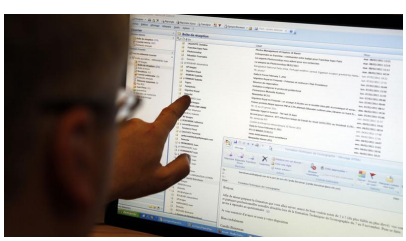
C'est mauvais signe.
Et dans le cas contraire ? Si votre mail figure dans la base de données de « Have I Been Pwned ? », c'est le moment de s'inquiéter. Les sites qui n'ont pas su vous protéger seront visibles dans un encart situé plus bas. Dans notre cas, l'une de nos adresses était utilisée sur deux sites qui ont été piratés en septembre et décembre 2015.
Si vous êtes inscrit sur l'un d'eux, sachez que des éléments complémentaires, comme la date de la fuite et la nature des données compromises (le mot de passe, le nom d'utilisateur ou l'activité sur le site web), sont donnés, lorsqu'ils sont connus.
HAVE I BEEN PWNED ?
À l'heure actuelle, « Have I Been Pwned ? » prend en compte 71 sites web ou applications et plus de 278 millions de comptes compromis. Parmi les services qui sont pris en compte figurent Adobe, Ashley Madison, Gmail, Snapchat, YouPorn, Battlefield Heroes ou encore Yahoo. Un classement liste également les dix piratages les plus spectaculaires.
*Reste une question, qui est tout à fait légitime : « Have I Been Pwned ? » n'est-il pas un site de façade qui ne servirait en fait qu'à inciter les internautes à donner leurs adresses web, dans le but de mener ensuite des **campagnes de hameçonnage** pour dérober encore plus de données personnelles ?*
*Dans sa **foire aux questions**, le site assure qu'aucune information de ce type n'est gardée en mémoire. Quant à la personne qui s'occupe de ce service, il s'agit d'un informaticien indépendant a priori digne de confiance, **Troy Hunt**. Celui-ci n'est pas un total inconnu : c'est un expert reconnu dans le milieu de la sécurité informatique et a été distingué par Microsoft.*

Réagissez à cet article

Source : *Un site pour vérifier si vos données ont été piratées – Tech – Numerama*

---

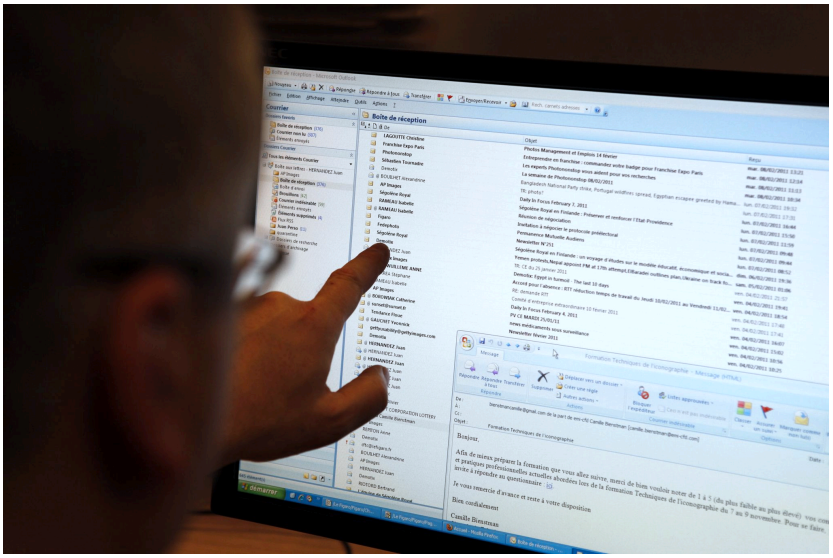
100 fois plus de victimes vol de données personnelles en deux ans en France



100 fois plus de victimes vol de données personnelles en deux ans en France

---

En 2015, cette pratique visant à dérober des informations personnelles par Internet ou par téléphone a fait plus de 2 millions de victimes en France. C'est cent fois plus qu'il y a deux ans.



Véritable piège pour les internautes, la pratique du phishing ne cesse de se répandre en France. Contraction de «fishing» (pêche) et «phreaking» (piratage de lignes téléphoniques), ce procédé malveillant vise à soutirer des données personnelles (mot de passe, identifiant de connexion, numéros de cartes bancaires). On parle également de «hameçonnage».

Sur la seule année 2015, plus de 2 millions de personnes auraient été victimes du phishing en France. C'est 100 fois plus qu'il y a deux ans, selon Europe 1 qui reprend un rapport de Phishing Initiative, site reconnu par les services de lutte contre la cybercriminalité. Le plus souvent, cette arnaque se manifeste par la réception d'un mail personnalisé provenant d'un organisme financier (banques), d'une entreprise (fournisseur d'Internet, EDF…) ou même d'une administration publique (CAF)… Du moins en apparence.

Car le message en question, aussi crédible et réaliste qu'il puisse paraître, vous invite en réalité à cliquer sur un lien, lequel vous redirige vers un site vous demandant de mettre à jour vos données personnelles. Dès lors, en se faisant passer pour des tiers, les cybercriminels à l'origine de ces mails frauduleux sont en mesure de récupérer vos informations personnelles. «L'augmentation des pratiques de phishing s'explique notamment par le nombre croissant de cybercriminels organisés en réseaux très structurés. D'autant que leurs méthodes sont de plus en plus sophistiquées. Auparavant, des fautes d'orthographe présentes dans les mails permettaient d'éveiller les soupçons. Désormais, c'est plus dur à déceler car ils paraissent davantage crédibles», explique Raphaël Renaud, spécialiste des questions liées au phishing.

Usurpées, les banques comme les grandes entreprises sont, elles aussi, directement concernées par le phishing. En modernisant leurs systèmes de sécurité, elles parviennent parfois à contrer les menaces. C'est le cas de Google qui a bloqué 7000 sites utilisés pour des attaques de phishing en 2015. De leur côté, les établissements bancaires assurent «un service de veille et donc une certaine publicité pour prévenir leurs clients, mais celle-ci est souvent insuffisante», remarque Serge Maître, secrétaire général de l'Association Française des Usagers des Banques (AFUB), avant de souligner que «le cryptogramme et le 3D Secure ont montré leurs limites face aux attaques de phishing.»

Comment réagir face au phishing?

S'il n'est pas encore trop tard, plusieurs méthodes permettent de contrer le phishing. Dans un premier temps, il est préférable de disposer d'un antivirus performant. Ensuite, «l'ultime chose à faire est de ne jamais cliquer dans un lien provenant d'un e-mail. Les services sérieux (banque, opérateurs téléphoniques, etc…) ne vous demandent jamais de changer un mot de passe de cette manière», explique Raphaël Richard avant d'ajouter «qu'il faut directement se connecter sur le site officiel pour ne pas avoir de doute». Enfin, certains sites tels que ou Phishing Initiative permettent de faire vérifier un mail en cas de soupçon mais également de signaler des adresses qui semblent suspectes.

En revanche, si un internaute vient d'être victime de phishing, il doit «déposer plainte si possible devant une brigade spécialisée dans les 48 heures car au-delà, cela devient plus compliqué. Il faut également contacter … [Lire la suite]

Réagissez à cet article

Source : *Données personnelles : le nombre de victimes de vol multiplié par 100 en deux ans en France*

Un phishing et Lastpass s’en est allé

Un phishing et Lastpass s’en est allé

Lors de la conférence Shmoocon, un chercheur a présenté une attaque de phishing particulièrement convaincante visant les services du gestionnaire de mot de passe Lastpass. En réaction, les mesures de sécurité ont été rehaussées par l'éditeur du service.

Le phishing n'est pas toujours un problème situé entre le clavier et la chaise. C'est en tout cas la thèse défendue par le chercheur Sean Cassidy, qui a présenté ce week-end lors de la conférence Shmoocon une attaque de cette catégorie particulièrement convaincante et capable de tromper les utilisateurs les plus aguerris du gestionnaire de mot de passe Lastpass.

L'attaque, baptisée « Lostpass » exploite plusieurs vulnérabilités présentes sur le service de gestion des mots de passe : il s'agit tout d'abord pour l'attaquant d'attirer l'utilisateur sur un site malicieux, puis d'afficher une notification indiquant à l'utilisateur que celui-ci a été déconnecté de Lastpass. Une fois celle-ci affichée, l'utilisateur est ensuite redirigé vers une page de login quasi identique à celle affichée par Lastpass en cas de déconnexion. L'attaquant peut exploiter un bug notamment présent dans Chromium afin de disposer d'un nom de domaine quasi similaire à celui utilisé pour les extensions chrome du même type que celles utilisées par Lastpass.

L'attaquant peut ensuite exploiter l'API ouverte de Lastpass pour vérifier si les identifiants entrés par l'utilisateur sont valides et pour savoir si celui-ci a activé un système d'identification à double facteur : si tel est le cas, l'attaquant peut également présenter une invite copiée sur celle proposée par le service de gestion de mot de passe et qui lui permet de récupérer par la même occasion le token généré par la double authentification. Une fois les identifiants récupérés, l'attaquant peut accéder au reste des mots de passe stockés par l'utilisateur, ou modifier les paramètres de sécurité du compte afin de faciliter d'éventuelles futures attaques.

Un problème entre la chaise et le clavier ?

Les équipes de Lastpass ont été mises au courant de ce scénario d'attaque au cours de l'été 2015 et ont depuis mis en place plusieurs mesures afin de protéger les utilisateurs. La société a ainsi mis en place un système de vérification par mail lorsque l'utilisateur se connecte depuis un appareil inconnu, ce qui permet selon Lastpass de réduire considérablement les attaques de ce type.

La société précise également revoir le fonctionnement de son extension :
celle-ci s'appuie en effet sur des notifications Viewport pour informer ses utilisateurs, une technique facile à imiter pour un attaquant qui souhaiterait tromper un utilisateur. Un comportement que Lastpass entend corriger afin de réduire un peu plus le risque de confusion entre véritables notifications et notifications malicieuses émanant du site visité.
Pour Sean Cassidy, le problème souligné par ce scénario est tout aussi critique qu'une vulnérabilité classique, mais celui-ci regrette que les attaques de type phishing soient trop souvent reléguées au simple rang des problèmes liés à l'utilisateur. Dans sa démonstration en effet, la différence entre les pages légitimes et les pages malicieuses utilisées par un attaquant est minime. Seule une infime différence de trois caractères dans une url et quelques différences typographiques séparent ici le vrai du faux, ce qui rend l'attaque bien plus inquiétante.

Réagissez à cet article

Source : *Lastpass : un phishing presque parfait*

50 attaques informatiques qui ont marqué le web Français en 2015

50 attaques informatiques qui ont marqué le web Français en 2015

Pendant qu'il est possible de lire un peu partout sur le web le « top 5 », le « top 7 » des attaques informatiques dans le monde, ZATAZ préfère regarder du côté de VOS ordinateurs avec le top 50 des attaques informatiques qui ont touché la France et les internautes francophones. Des cas traités par ZATAZ.

Madison, Hacking Team, Hôtels Trump, Madisson, Vtech… les cas de piratage et de fuites de par le monde ont été pléthoriques, encore une fois, cette année. Revenir sur ces cas, pourquoi pas, mais il suffit d'en parler aux internautes francophones croisés sur la toile pour se rendre compte qu'ils ne se sentent pas concernés, et considères ces actes comme « drôles », ou « insignifiants » pour leur vie 2.0. Bilan, sur 1 475 personnes interrogées par ZATAZ (Âgés de 18 à 55 ans – entre le 22 décembre et le 30 décembre – 71% d'hommes – 43% évoluant dans le monde de l'informatique) seules 96 personnes interrogées avaient pris soins de modifier leurs mots de passe, car utilisés plusieurs fois dans des comptes différents (webmails, forums, …). 27 des interviewés confirmaient qu'ils regardaient plus souvent leur compte en banque. 339 avaient décidé, cette année, de faire un backup mensuel de leurs données (Je vous conseille fortement de pratiquer une sauvegarde, chaque jour, ndr).

Opération Anti Charlie

Janvier 2015, les attentats contre la rédaction de Charlie Hebdo et une supérette parisienne met en émoi le monde et le web. Les Anonymous décident de s'attaquer aux sites de djihadistes. Les participants s'attaquent à tout et n'importe quoi, dont des commerces de produits Hallal. En réponse, de jeunes internautes musulmans et plus d'une centaine de pirates du Maghreb et d'Asie lancent l'Opération Anti Charlie. Plus de 20 000 sites en .fr sont modifiés et/ou infiltrés. A noter que certains sites piratés, mais aussi infiltrés sans que la moindre trace du piratage n'apparaisse publiquement, ne sont toujours corrigés 11 mois plus tard. Une attaque informatique qui, sous l'excuse d'une cyber manifestation, était surtout menée et manipulée par des commerçants officiant dans le blackmarket. Dans la liste des espaces touchés : plusieurs centaines de sites du CNRS et des Restaurants du cœur, ainsi que 167 établissements scolaires d'Aquitaine ou encore de vieux espaces du Ministère de l'Intérieur et de la Défense.

TV5 Monde

Avril, le piratage de TV5 Monde fait grand bruit dans un contexte politique tendu. Au début du mois d'avril, la chaîne fait face à une cyberattaque d'ampleur. Ses différents comptes de réseaux sociaux sont piratés et diffusent de la propagande de la secte de Daesh. La diffusion des émissions de la chaîne sont coupées de l'antenne par la direction. Trend Micro évoque l'implication possible d'un groupe d'APT d'origine russe, Pawn Storm. Les autorités restent discrètes sur les différents éléments de l'affaire, si bien qu'encore aujourd'hui, on peine à se faire une idée de ce qu'il s'est vraiment passé dans le SI de France TV5 Monde. C'est surtout l'impact médiatique de cette attaque que l'on retiendra. Cinq mois après l'attaque, ZATAZ alertera l'ANSSI et TV5 Monde pour corriger d'autres failles informatiques découvertes sur les serveurs de la chaîne. A noter qu'un internaute est arrêté au mois d'août en Bulgarie. Des documents retrouvés dans son ordinateur son signé CyberCaliphate, le pseudonyme utilisé lors de l'attaque de TV5 Monde.
Un piratage qui fait ressortir que les media Français sont totalement dépassés par les potentialités malveillantes qui planent au-dessus de leurs claviers. Pour preuves, les différentes fuites de données et autres failles remontées par ZATAZ auprès de France Télévision [Fuite de données de téléspectateurs] ; du journal telecablesat.fr et 13 833 comptes clients volés.

Infiltrations

Les banques, les grands groupes Français sont visés, chaque jour, par des tentatives de piratage. Des attaques réussies ou non. Les clients ne sont jamais informés. Pendant ce temps, des millions d'informations appartenant aux Français sont pillés, copiés, revendues sur la toile. Par exemples, avec trois espaces de filiales de la BNP Paribas. Des sites retrouvés dans un espace pirate. Les malveillants s'échangeant les failles donnant accès à des bases de données. ; le pétrolier Total, et sa boutique, attaquée et pillée en janvier 2015. 29.657 clients d'un espace commercial grand public du pétrolier. Les pirates m'avouaient avoir vendu pour 500€ des informations de Français collectés dans cette BDD. Des fuites de données accessibles directement, ou via des tiers commerciaux, comme ce fût le cas pour TF1 et 1,9 millions de clients Français, abonnés à des journaux papiers ; Le site Internet La Boutique Officielle, spécialisé dans la vente de vêtements « Urban », visité par des pirates informatiques. Données des clients volées. L'entreprise ferme son espace numérique plusieurs jours ; de son côté, la CNIL contrôle 13 sites de rencontres français, 8 sont mis en demeure de mieux contrôler les informations de leurs « clients » ; En Mars, une faille informatique permettait à un pirate informatique de mettre la main sur les données d'un espace Orange Business.
Juin 2015, le portail Associations Sportives, qui répertorie plus de 240.000 clubs et associations françaises est infiltré. Le pirate diffuse un extrait de la base de données. Même sanction pour l'enseigne King jouet qui corrigera une fuite de données visant ses clients. Quinze ans de factures disponibles sur le web d'un simple clic de souris ; Un pirate informatique annonçait, en septembre, le vol des données appartenant au laboratoire Santé Beauté. Le groupe Santé Beauté regroupe des marques telles que « Barbara Gould », « Linéance », « Email diamant », « Batiste », « Nair », « Poupina » et « Femfresh ».
En octobre, le piratage de plusieurs espaces de la marque de lingerie ETAM était annoncé. Le jeune pirate diffusait plusieurs captures écrans qui ne laissent rien présager de bon pour la marque de textile.

Ransomwares

La grande mode des logiciels dédiés au chantage 2.0 (blocage de disque dur, chiffrement de données, NDR) aura frappé très fort en cette année 2015. ZATAZ a reçu pas moins de 3.022 mails de personnes et de PME piégés par ce genre d'attaque informatique. J'ai pu référencer plusieurs dizaines de mairies ou entités publiques malmenées par un ransomware, comme GDF Suez.

Arnaques et autres fraudes

Des arnaques au ransomware qui oblige les « pirates » à payer pour récupérer leurs informations prises en otage. Des arnaques qui existent aussi sous d'autres formes, comme la fraude au président. KPMG, Michelin, le Printemps, LVMH, Vinci, Total, Brevini, Areva, le cabinet d'avocats Baker & McKenzie, Finder France, SAM, Abuba, Vallourec, Sonia Ryckiel, Dargaud, Seretram… quelques exemples d'entreprises qui ont versé de l'argent à des professionnels du social engineering. Des pirates qui avaient collecté un grand nombre d'informations sur l'entreprise. Des données qui vont permettre de convaincre les services comptables de verser des millions d'euros aux pirates. Ces derniers se faisant passer pour le patron, un client, un fournisseur. Les premières arrestations ont eu lieu en février 2015. Elles concernaient les pirates ayant jeté leurs dévolus sur le club de football de l'Olympique de Marseille (OM). Deux hommes (50 et 34 ans) seront été arrêtés à Tel-Aviv.
Autre chantage, autre arnaque, celle mise en place par Rex Mundi. Plus de 15 000 identités de patients d'un laboratoire de santé français diffusées par le pirate. Le maître chanteur réclamait 20.000€ contre son silence. Le laboratoire n'a pas payé. Les informations sensibles et privées des patients seront diffusées.
Des pirates informatiques qui se spécialisent, même dans les prénoms à l'image de cet arnaqueur qui ne visait que les « Jacquelines« . Un prénom que l'escroc considère comme étant celui de personnes âgées.
Le chômage et la « crise » économique profitent aux pirates. Comme avec le site Internet Crédit Financement Fiable qui cachait une escroquerie numérique ; ou encore avec plusieurs cas d'arnaques téléphoniques. Le pirate se faisant passer pour la FNAC, Conforama ou encore Darty ; Les hôteliers, les chambres d'hôtes ne sont malheureusement pas oubliés avec une vague massive de fausses réservations de séjours.

Universités et écoles

Piratage, spams massifs, infiltration par des pirates présumés Chinois et maintenant, la diffusion d'une base de données d'élèves. L'informatique de l'université de Lyon 3 était-elle devenue complétement folle en février 2015 ? Quelques mois plus tard, rebelote, avec de nouvelles fuites de données. D'autres grandes écoles seront visées par des fuites, comme l'extranet du groupe éducatif ESG fermé à la suite d'un piratage informatique ; ou encore le cas de milliers de documents privés, et pour certains sensibles, d'étudiants de l'EPITECH. Plus de 47 000 dossiers pour quatre ans de fuite.

Fuite de données d'adresses postales

En Mars 2015, via le site Internet Degrouptest, il était possible de trouver l'adresse postale collée à un numéro de téléphone. Même une ligne téléphonique sur liste rouge pouvait être démasquée ; Neuf mois plus tard, le même type de fuite touchait un site Bouygues Telecom. Ici aussi, il suffisait de rentrer un numéro de téléphone pour accéder aux adresses postales. Liste rouge comprise.
Des fuites de données que connaitra aussi la société Somfy (spécialiste de la domotique). Zataz.com a pu constater que l'un de ses espaces web, il était dédié au personnel de l'entreprise, avait été infiltré par de nombreux pirates informatiques. Des pirates qui s'étaient empressés d'installer des backdoors, des portes cachées, leur permettant de jouer, à loisir, avec le serveur et son contenu.
Fuite de données sous forme de CV aussi, comme ce fût le cas pour un site d'Ametix. Des milliers de CV sauvegardés directement dans un dossier du WordPress d'un site dédié à une opération marketing.

Viagra et baskets dans votre site web

Le Black Seo, l'utilisation malveillante du référencement de liens et pages pirates via un site légitime, aura permis à des escrocs d'installer de fausses pharmacies et autres boutiques de contrefaçons dans des centaines de sites Français. Des Mairies, des boutiques, des sites étatiques ; Sans parler des sites propres sur eux, capable d'attirer dans leurs filets des milliers de Français, comme la fausse boutique officielle Nike RBFIRM.
En juin, le site Internet officiel de la chambre des Huissiers de Justice de Paris est (le site diffuse toujours des liens malveillants, ndr) piraté et exploité par des vendeurs de viagra ; des attaques que zataz révélera aussi en août 2015 à l'encontre du site de la Haute Autorité de la Santé ; ou encore en septembre pour la Fédération nationale des associations d'accueil et de réinsertion sociale, pour le portail dédié à une étude médicale en France et l'Établissement de Préparation et de Réponse aux Urgences Sanitaires (APRUS).

DDoS

Bloquer un site Internet, un serveur, un streamer (joueur en ligne) … la grande mode des petits pirates, en 2015. Des attaques qui ont eu pour mission de bloquer un site, d'empêcher son bon fonctionnement. Cette année, le groupe de presse belge Rossel (Le soir, La Voix du Nord, …), mais aussi NRJ, BFM, l'Académie de Grenoble ou encore l'UMP ont été attaqués de la sorte.
Des attaques faciles à mettre en place pour le premier idiot qui passe. Les boutiques vendant du DDoS poussent comme les champignons à l'automne. A noter que durant ce mois de décembre 2015, de très nombreux amateurs de jeux en ligne, des streamers, se sont retrouvés menacer par un maître chanteur demandant de l'argent pour stopper ses blocages.

Cartes Bancaires

La fraude à la carte bancaire se porte bien ! La police de Toulouse, et plus précisément la SRPJ, a mis la main sur trois cinéphiles pas comme les autres au mois d'avril 2015. Les individus avaient piégé un distributeur de billets installé dans le cinéma Gaumont Wilson ; En Juin, la banque postale déposé plainte après que des distributeurs de billets soient piégés par des skimmeur, du matériel pirate capable d'intercepter les données inscrites sur une carte bancaires ; Des cartes bancaires qui sont devenues causantes, en mode sans fil. Bilan, même le CNRS a tiré la sonnette d'alerte en indiquant que les cartes de paiement sans contact comportent de graves lacunes de sécurité ; du sans fil qui attire, en novembre, les Frotteurs 2.0 dans le bus, le métro et autres lieux publiques ; du matériel pirate que l'on a retrouvé, entre autre, au mois d'août 2015, dans un parking proche de la gare Montparnasse (Paris). Et les arrestations se succèdent, comme à Tours, et de la prison ferme (7 mois) pour l'un de ces pirates.

Objets connectés

En Mai, je vous expliquais que pour moins de 40 euros, des voleurs de voiture s'invitaient dans les véhicules que les propriétaires pensaient avoir fermé. Même le Ministère de l'Intérieur Français s'en inquiètera quelques jours plus tard ; des panneaux d'affichage seront attaqués, modifiés (Lille, Paris…). De la geek security attitude qui démontre aussi et surtout la faiblesse des villes connectées. La partie immergée d'un problème qui pourrait être bien plus dramatique.

Swatting

Le swatting, une mode venue des Etats-Unis. L'idée du pirate, envoyer les forces de l'ordre au domicile d'un joueur en ligne. En juillet, un second cas de swatting touchait la France. Domingo est un jeune Youtuber/Streamer. Un de ces jeunes professionnels du jeu en ligne qui diffuse ses parties, en direct. Il s'est retrouvé nez-à-nez avec la police après ce genre de mauvaise blague ; Le premier cas, en février 2015, BibixHD. L'action de la police, à son domicile, sera diffusé en directe alors qu'il était en train de jouer au jeu DayZ. Un inquiétant jeu qui amuse des adolescents en mal de repères. Certains vendant des possibilités de swatting pour quelques euros comme je le révélais au moins d'août !

Phreaking

Le piratage téléphonique, le phreaking, un acte numérique qui ne connait pas la crise. Mission du pirate, mettre la main sur une ligne téléphonique qu'il pourra commercialiser, surtout les minutes disponibles d'appels. Par exemples, en juillet, 5.288€ de détournement téléphonique pour la Maison de la Jeunesse de Nancy. En novembre, 43 000€ d'appels téléphoniques détournés pour le département des Deux-Sèvres.

Heartbleed

En juillet, la faille Heartbleed refaisait surface dans mes recherches. Une vulnérabilité datant d'avril 2014. Plusieurs centaines d'importants serveurs Français étaient toujours faillibles, 16 mois plus tard.

Scientologie

Des Anonymous se sont attaqués à plusieurs sites Français de la secte de la scientologie. Les manifestants 2.0 ont voulu rappeler l'affaire de Gloria Lopez, une ancienne scientologue retrouvée morte en 2006.

Box

Cette année, nous aurons connu chez ZATAZ cinq cas, dont deux considérés comme sérieux. Numéricâble, et Bouygues. Ce dernier avait son option Playin'TV particulièrement sensible. Plusieurs problèmes qui auraient pu servir à des actions malveillantes.

Réagissez à cet article

Source : *ZATAZ Magazine » Les 50 attaques informatiques qui ont marqué le web Français en 2015*

URGENT : Phishing Free Mobile, ne vous faites pas avoir !

URGENT : #Phishing Free Mobile, ne vous faites pas avoir !

Réagissez à cet article

Source : *URGENT : Phishing Free Mobile, ne vous faites pas avoir ! – Le Blog du Hacker*