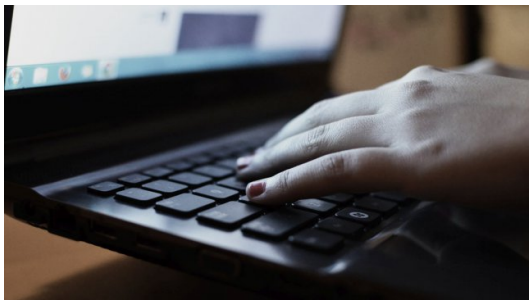
Arnaque à la SexTape – Ne vous découvrez pas d’un clic

	Arnaque à la SexTape – Ne vous découvrez pas d’un clic

Mélange de Sexe et d'Extorsion, la Sextorsion, autrement dit l'utilisation du sexe pour faire chanter des internautes, est un phénomène qui prend de l'ampleur sur internet. Le 24 février dernier, un garçon de 13 ans qui habite en Haute-Vienne près de Limoges a ainsi été contacté sur Internet.

Le 24 février dernier, un garçon de 13 ans qui habite en Haute-Vienne près de Limoges a ainsi été contacté sur Internet. Une « prétendue » jeune fille l'a abordé sur les réseaux sociaux et l'a encouragé à se déshabiller devant sa webcam puis lui a demandé 150 € en mandat-cash sous peine de diffuser la vidéo. Une grosse frayeur pour l'adolescent qui a eu le bon réflexe de prévenir ses parents.
D'abord abordé puis dragué, le mode opératoire est bien rodé pour ces cyberdélinquants et peut toucher la plupart d'entres vous.

Adultes ou adolescents, ils sont de plus en plus nombreux à tomber dans le piège

LA TECHNIQUE
1- Repérage
La technique consiste à repérer ses victimes sur des sites renfermant des nids de cibles faciles. Les forums, les réseaux, sociaux, les sites de rencontre, les sites de loisirs et de manière générale tous les sites internet favorisant le dialogue, les rencontres amicales et surtout amoureuses sont les plus couramment utilisés.
Ca ne fait pas peur au prédateur d'aborder dans la même journée plusieurs dizaines de cibles. L'essentiel est d'avoir un minimum quotidien de victimes pour s'assurer un revenu minimum et régulier.
Trouver des victimes sur Internet pourrait bien finit un jour, comme les envois en masse de mailings ou des opérations en masse de phoning, par avoir ses propres statistiques de retour (Un pourcentage assuré de victimes par rapport au nombre de cibles).

2- Le contact
Une fois la cible repérée, il faut la vérouiller.
Si la cible est un homme, l'usurpateur prendra la peau (les photos et les vidéos) d'un modèle de beauté féminin; et si la cible est une femme, c'est à un bel étalon ou quelqu'un excessivement attentionné que le pirate ressemblera. Il n'y a que l'embarra du choix sur Internet. Un simple clic droit sur une photo permet de l'enregistrer sur son ordinateur et ensuite de l'utiliser impunément.
Le dialogue est alors très dirigé, cherchant à faire parler la victime d'elle, la complimentant, lui trouvant un nombre important de points communs (ça fait partie des techniques de manipulation comportementale que ces voyous savent très bien uiliser) cherchant à instaurer un climat de confiance, développer de la complicité et surtout faire baitre, **DES SENTIMENTS** !
Ne vous en faites pas pour le malfrat, quoi qu'il vous dise, il n'a de son coté aucun sentiment, il atend juste que des sentiments commenent à naitre chez sa proie et on peut alors considérer qu'elle est malheureusement vérouillée.

3- Le piège
Il existe une technique similaire consistant à vous dérober de l'argent et parfois même, des montants faramineux. Mais c'est la tournure d'une arnaque à la SexTape que prendra la relation à distance si vous avez une Webcam.
Rapidement, au bout de quelques heures ou quelques jours, une fois les sentiments vous faisant quitter le monde rationnel mais plutôt voyager dans le monde des émotions, votre interlocuteur, le plus beau ou la plus belle du monde vous invite à vous dévoiler physiquement pour son plus grand bonheur… Une démarche plus ou moins naturelle vous me direz, dans le cadre d'une relation amoureuse qui commence à s'installer…
Cependant, à l'autre bout de la souris, l'interlocuteur malintentionné est prêt à appuyer sur sa gachette pour …. vous enregistrer en train de vous dénuder, en train de jouer.
Une fois cette étape franchie, le piège s'est refermé et votre interlocuteur ou votre fausse interlocutrice détient précieusement des images compromettantes.

4- Le chantage
Une fois le piège refermé sur vous, et cette étape franchie, le cybercriminel s'empresse de mettre fin au jeu sexuel pour le remplacer par un jeu de force, consistant à vous menacer de dévoiler sur Internet d'envoyer à votre famille, à votre employeur ou à d'autres de vos contacts la vidéo ou les photos compromettantes capturées si vous ne payez pas une somme d'argent. C'est du chantage (action d'extorquer de l'argent ou tout autre avantage par la menace, notamment de révélations compromettantes ou diffamatoires).
Les pirates vous demanderont à tous les coups, pour conserver l'anonymat grace à des complices, de régler par mandat cash, westernu union ou par monnaie électronique, naturellement anonyme.

5- Que faire pour s'en protéger ?
L'action la plus citoyenne que vous pourriez faire consisterait à nous aider à faire de la prévention en partageant cet article, en parlant à votre entourrage ou à vos proches de l'existence de ce fléau pour éviter qu'ils se fassent attraper, car une fois le piège refermé sur vous, vu que les communicatins peuvent être surveillées, enregistrées, sauvegardées et partagées dans le cloud, il est souvent trop tard pour supprimer toutes traces de photos ou vidéos compromettantes et ceci, même si vous payez la rançon…
Quelques conseils
• Sois méfiant à l'égard de ceux qui veulent en savoir trop.
• Ne donne aucune information sur toi ou sur ta famille (comme ton nom, ton numéro de téléphone, ton adresse ou celle de ton école…) sans en parler avec tes parents.
• Si tu reçois ou si tu vois quelque chose qui te met mal à l'aise, ne cherche pas à en savoir plus par toi-même, déconnecte toi et parles-en à tes parents.
• Si tu envisages de rencontrer quelqu'un que tu as connu en ligne n'y va jamais sans en parler à tes parents.
• Supprime, sans les ouvrir, les mails que tu n'as pas demandés ou qui te sont envoyés par des personnes en qui tu n'as pas confiance.
• N'achète jamais rien sur Internet, sauf si tes parents sont avec toi pour te conseiller.
• Ne donne jamais un mot de passe.

6- Et si c'est trop tard
Si c'est malheureusement trop tard pour vous et que vous êtes bel et bien victime d'arnaque à la Sex Tape, il faut surmonter sa honte et en parlet à des amis ou des confidents. Si vous êtes mineur, parlez-en immédiatement à vos parents. Il faut relativiser, se dire que ce n'est pas catastrophique. Vous êtes juste victime d'une escroquerie.
Ensuite, il est important que pouvoir récolter le maximum d'éléments techniques qui permettront de remonter jusqu'à l'auteur de cette machinerie. Pseudos, courriers électroniques avec leurs entêtes, récupérer les adresses IP, garder les SMS, etc…. seont un point de départ solide pour une enquête.

Il est également important de porter plainte.
Si vous n'avez pas encore payé, malgré les menaces ou la diffusion de vidéos, ne le faites surtout pas. Payer n'engagera pas la personne à supprimer les informations compromettantes.
Si vous pensez avoir été victime d'une escroquerie sur Internet, mais n'êtes pas sûr, si vous voulez des conseils suite à une tentative d'escroquerie dont vous auriez été victime, vous pouvez contacter la plateforme téléphonique Info Escroqueries, où des policiers et des gendarmes vous répondent au 0811 02 02 17 (coût d'un appel local) », porter plainte en brigade de Gendarmerie ou au Commissariat de Police ou bien signaler l'acte malveillant dont vous êtes victime sur la plateforme PHAROS (Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements) sur www.internet-signalement.gouv.fr.

Ces escroqueries sentimentales sont souvent organisées, par des réseaux structurés, depuis des pays d'Afrique, où la justice peine à se faire entendre même si le cyber harcèlement est puni en France par l'article 222-33-2-2 du code pénal (2014) de 2 ans à 3 d'emprisonnement et de 30 000 à 45 000 € d'amende.

Réagissez à cet article

Auteur : Denis JACOPINI

Sources :

http://lci.tf1.fr/france/faits-divers/escroquerie-a-la-sextape-sur-le-net-comment-reagir-6280167.html

http://france3-regions.francetvinfo.fr/limousin/haute-vienne/cybercriminalite-un-jeune-limousin-victime-de-sextorsion-937350.html

https://www.internet-signalement.gouv.fr

Gare aux « tarifs délirants »

des numéros en 118

Gare aux « tarifs délirants » des numéros en 118

Les numéros de renseignements téléphoniques comme le « 118 218 » existent encore, et ils sévissent auprès d'usagers fragiles, mal informés ou pressés… qui en paient le prix fort.

Des numéros de renseignements téléphoniques, la plupart d'entre vous n'en connaissent que le duo moustachu qui amusait la galerie dans les spots TV voilà quelques années. À force de le répéter sur un air de générique des années 80, le numéro « 118 218 » s'est peut-être inscrit durablement chez certains. Ce que l'on sait moins, c'est que cette société – leader du marché – ainsi que ses pairs, génèrent une « vague de plaintes » des utilisateurs.

L'association 60 Millions de consommateurs dit avoir reçu un certain nombre de réclamations de personnes ayant vu leur facture téléphonique exploser suite à un appel en « 118 ». Après la libéralisation complète du « 12 » en 2007, ces services se sont mis à pulluler. Depuis, la plupart a disparu et le nombre d'appels a fondu, mais une dizaine survit. Le 118 218, de la société Le Numéro (filiale de l'américain KGB), a même lancé son application.

Une arnaque en 3 leçons

« Pour à peine 2 minutes et 40 secondes au bout du fil, un de nos lecteurs s'étonne d'avoir payé 10,80 euros au 118 218 », rapporte l'association. Elle voit trois explications. La première : « Face à la baisse des appels, les services de renseignements téléphoniques ont augmenté leurs tarifs jusqu'à des sommets inédits. La plupart facturent désormais 5 à 6 euros la première minute d'appel, puis 2,50 à 3 euros les minutes suivantes. »

En effet, les services de renseignements téléphoniques « sont les seuls numéros surtaxés pour lesquels la réglementation ne fixe aucun plafond tarifaire », rappelle 60 Millions de consommateurs, alors que les autres numéros à tarification majorée (08) ont plafonnés à 0,80 euro la minute depuis la réforme d'octobre 2015.

Réagissez à cet article

Source : *Gare aux « tarifs délirants » des numéros en 118*

Un site Internet pour le règlement en ligne des litiges

Si vous avez un problème concernant un achat en ligne, vous pouvez utiliser ce site pour essayer d'obtenir un règlement extrajudiciaire.
Pour l'utiliser, vous devez vivre dans l'Union Européenne et le professionnel concerné doit y être établi
Les professionnels de certains pays peuvent également utiliser ce site pour déposer plainte contre un consommateur concernant un bien ou service vendu en ligne. … [Lien vers le site https://webgate.ec.europa.eu]

Réagissez à cet article

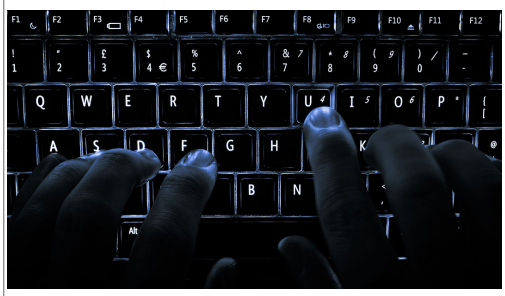
Source : *Accueil – Règlement en ligne des litiges*

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.

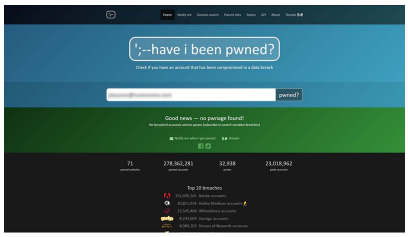
Autre méthode, celle du défaçage.
Cette dernière vise à modifier un site web en insérant du contenu non désiré par le propriétaire. Cette méthode est employée par les hackers militants qui veulent dénoncer les pratiques de certains gouvernements ou entreprises. Pour ce faire, le hacker exploite une faille 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.

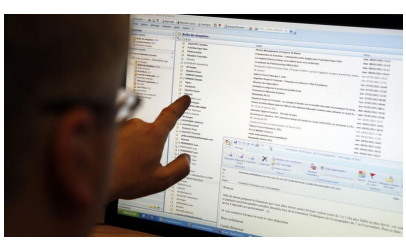
C'est mauvais signe.
Et dans le cas contraire ? Si votre mail figure dans la base de données de « Have I Been Pwned ? », c'est le moment de s'inquiéter. Les sites qui n'ont pas su vous protéger seront visibles dans un encart situé plus bas. Dans notre cas, l'une de nos adresses était utilisée sur deux 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*

---

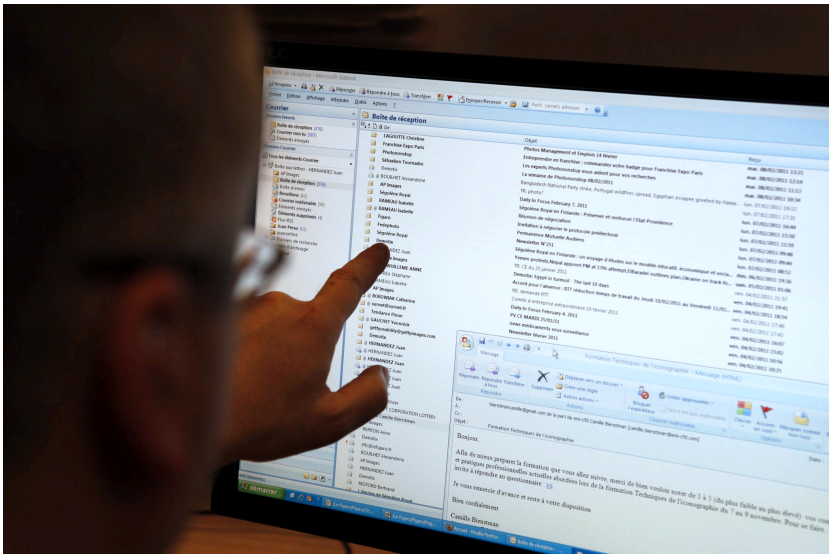
100 fois plus de victimes vol de données personnelles en deux ans en France



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*

Une Vauclusienne se fait escroquer de 23000 euros par téléphone

Une Vauclusienne se fait escroquer de 23000 euros par téléphone

---

Difficile de faire plus simple comme escroquerie : une fausse avocate a escroqué une habitante du Vaucluse de près de 23000 euros par de simples appels téléphoniques

En décembre dernier, la faussaire appelle cette habitante de Saint-Romain en Viennois, près de Vaison-la-Romaine, qui vient de perdre son père, pour lui annoncer qu'il avait contracté une assurance-vie à son bénéfice.
Pour toucher les 127 000 euros de capital, elle doit d'abord payer 9500 euros d'honoraires. Elle s'exécute, après avoir reçu des documents convaincants par mail, et fait un virement… en Lituanie. Quelques jours plus tard, rebelote, cette fois avec un virement de près de 13500 euros en Bulgarie. «Il lui faudra encore quelques jours pour se douter d'une entourloupe.
Elle s'adresse alors à sa banque, qui lui confirme qu'elle a été escroquée», raconte le journal. Un stratagème simple, qui rappelle «l'arnaque au PDG», dont sont victimes depuis plusieurs années de nombreuses entreprises françaises.

Réagissez à cet article

Source : *Une Vauclusienne se fait escroquer de 23000 euros par téléphone*

Plusieurs escrocs sur

Leboncoin écopent de peines de prison

Plusieurs escrocs sur Leboncoin écopent de peines de prison

Les autorités utilisent Leboncoin pour surveiller les escrocs qui revendent du matériel volé. Plusieurs forces de police indiquent avoir réussi à arrêter des auteurs présumés, certains ont même été condamnés à des peines de prison.

Comme bon nombre de plates-formes de vente en ligne, Leboncoin.fr peut servir pour des escrocs de moyen d'écouler une marchandise indûment obtenue voire d'appâter des victimes. En région parisienne, un groupe de personnes vient d'être condamné à des peines de prison pour avoir revendu des voitures sur le site.
Ces véhicules d'occasion étaient achetés avec de faux chèques de banque pour les revendre, 30 à 40 % moins cher que l'argus, contre des espèces. Des annonces étaient régulièrement publiées sur Leboncoin puis rapidement retirées, une fois la vente conclue. Au total, 71 automobiles ont été répertoriées par les forces de police.
Selon Le Parisien, les escrocs ont pu être repérés notamment grâce aux annonces publiées sur le site.
Le cerveau du réseau, un homme de 28 ans, écope d'une peine de 5 années de prison dont 1 an avec sursis avec mise à l'épreuve. Il devra en outre rembourser les victimes. Les autres membres ont été condamnés par le tribunal correctionnel de Pontoise à 4 et 2 ans de prison (associées à des peines de sursis).

Le site internet leboncoin.fr

Un voleur arrêté après avoir mis des annonces sur Leboncoin
En Bretagne, les autorités indiquent avoir interpellé un homme soupçonné d'avoir dérobé du matériel de jardinage auprès d'une enseigne locale. L'individu a volé des objets pour un préjudice total estimé à 2 500 euros puis a tenté de revendre une partie du butin sur Leboncoin, sans se soucier que le vendeur ou la gendarmerie surveillerait la plate-forme.
Dans les jours suivants le délit, le responsable du magasin qui avait subi le vol a trouvé une annonce pertinente. « Nous avons ensuite travaillé à partir de cette annonce, puis nous sommes remontés jusqu'à l'auteur présumé des cambriolages », explique le maréchal des logis-chef Goby auprès du quotidien Ouest-France.
Le domicile de la personne a été perquisitionné et nombre d'objets dérobés s'y trouvaient. L'affaire a été transmise au parquet de Brest, où sera jugé l'auteur présumé.

Réagissez à cet article

Source : *Plusieurs escrocs sur Leboncoin écopent de peines de prison*

Les 5 dangers pour vos ordinateurs, smartphones et données en 2016

Les 5 dangers pour vos ordinateurs, smartphones et données en 2016

Les 5 tendances qui motiveront leurs actions envers votre ordinateur, votre smartphone, vos données…

Ecartelée entre la démocratisation de l'Internet des objets (thermostat intelligent, balance connectée…), la prise de pouvoir du stockage dans le « cloud » et l'émergence des nouveaux smartphones vedettes, la sphère des nouvelles technologies subira en 2016 les assauts des virus virulents, des arnaques en ligne, des cybercriminels.
Comme un caméléon virtuel, la cybercriminalité s'adaptera plus que jamais à l'air du temps pour exploiter les nouveaux territoires en friche.
Entre prudence et clairvoyance, voici les 5 tendances cybercriminelles qui se développeront ces 12 prochains mois, selon les experts de l'éditeur de solution de sécurité BullGuard.

1. La montée en puissance du « ransomware »
Impitoyable méthode d'extorsion, le « ransomware » bloque votre ordinateur, crypte vos fichiers personnels et vous réclame un paiement en ligne pour les libérer.
La menace brandie en cas de refus de payer la rançon : l'extermination de vos données (photos, vidéos, documents…).
Alors que les virus à l'ancienne et les chevaux de Troie accusent une certaine perte de vitesse, le « ransomware » est appelé à les dribbler.
Ces logiciels malveillants s'attrapent en visitant un site préalablement « hacké » (piraté) ou un obscur site volontairement malveillant, en téléchargeant des fichiers vérolés, notamment sur les plateformes d'échange de fichiers illégaux…

2. Le smartphone, cette cible indiscrète
Connecté à Internet 7 jours sur 7, 24 heures sur 24 dans le scénario le plus extrême, le smartphone concentre une myriade de données personnelles, des adresses email de vos contacts au numéro de votre carte de crédit.
Le téléphone est par conséquent une cible de choix pour les cybercriminels, qui rivalisent d'ingéniosité pour contourner les nouvelles barrières de sécurité régulièrement déployées par Apple pour ses iPhone et Google pour son système d'exploitation mobile Google Play.
Après avoir concentré leurs efforts sur la Chine et l'Extrême-Orient, les cybercriminels devraient viser tout particulièrement l'Europe en 2016.
Certes, nos smartphones étaient déjà menacés par le virus et les logiciels malveillants. Hélas, le niveau d'alerte devrait grimper de quelques degrés.

3. L'Eldorado inquiétant de l'Internet des objets
Nouvelle marotte des constructeurs, l'Internet des objets entend envahir notre quotidien pour évaluer et prédire nos besoins, mesurer notre activité, adapter l'éclairage et le chauffage de notre habitation en fonction de nos usages…
Qu'il s'agisse d'un pèse-personne connecté ou d'un thermostat intelligent, ces appareils vulnérables de par leur connexion constante à Internet récoltent au kilo les données personnelles.
Imaginons le cas d'une caméra de sécurité connectée. Elle pourrait simplement être détournée par un cybercriminel pour détecter les moments où vous quittez votre maison.
Toujours en quête d'un standard, notamment pour la sécurité, la galaxie de l'Internet des objets, tout juste née de son Big Bang historique, ne manquera pas de révéler en 2016 ses failles et ses vulnérabilités.

4. Des nuages dans le ciel du « cloud »
Inexorable lame de fond qui modifiera à jamais le monde du stockage, le « cloud » éparpille données et fichiers dans un nuage de serveurs (ordinateurs) répartis dans d'immenses « data center » aux quatre coins du monde.
Ces « fermes » informatiques dédiées au stockage et au traitement des données présentent un double intérêt pour les cybercriminels.
Leur puissance peut être détournée à d'autres fins, tandis que les données stockées constituent un sérieux trésor de guerre au cœur duquel il est tentant de piocher.
Objet de toutes les attentions des esprits mal intentionnés, la vulnérabilité du « cloud » risque d'être régulièrement soulignée ces prochains mois.

5. Les gangs sous les projecteurs
Les cybercriminels se structurent en gangs d'une efficacité redoutable, souligne BullGuard.
« Ils passent des semaines, voire des mois, à effectuer des missions de reconnaissance avant d'attaquer des organisations », témoignent les experts de l'éditeur. « Ces entreprises ont été conçues dès le départ pour se spécialiser dans les crimes informatiques et ont des hiérarchies cloisonnées qui incorporent des programmeurs spécialisés dans le piratage, de vendeurs de données et des gestionnaires, tous supervisés par un cadre supérieur. Ces équipes de cybercriminels occuperont le devant de la scène en 2016. »

Réagissez à cet article

Source : *Virus, arnaques en ligne, cybercriminalité : les 5 dangers de l'année 2016 – L'Avenir Mobile*

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*