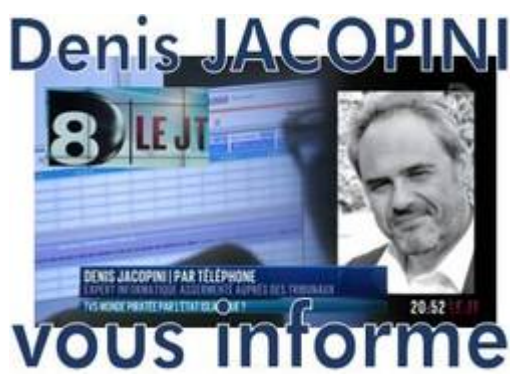
Réseaux sociaux, messageries, jeu vidéo… Comment les terroristes communiquent ?



Réseaux sociaux, messageries, jeu vidéo… Comment les terroristes communiquent ?

Les jihadistes utilisent abondamment les outils numériques de communication. Problème : ceux-ci sont de plus en plus difficiles à surveiller.

Les terroristes islamistes utilisent depuis toujours les outils numériques de communication qui présentent l'avantage d'être simples pour des personnes n'ayant pas de compétences particulières tout en étant terriblement puissants :
• Les réseaux sociaux pour la propagande publique (Youtube, Facebook, Twitter, etc.
• Les applis de messagerie et de voix sur IP pour la communication interpersonnelle (WhatsApp, Snapchat, Skype, iMessage, Viber, Telegram, etc.)

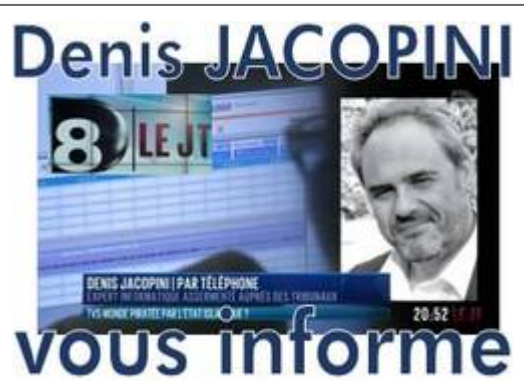
Même le jeu vidéo
Les terroristes utiliseraient même le jeu vidéo. C'est une information livrée avant les attentats de Paris par le ministre de l'Intérieur belge. Selon lui, la Playstation 4 serait exploitée pour communiquer vocalement via l'appli de voix sur IP intégrée au réseau PSN (PlayStation Network).
D'après Jan Jambon, ces communications seraient « plus difficiles à écouter que WhatsApp ». Les terroristes pourraient aussi faire passer de courts messages à des complices via les jeux eux-mêmes, par exemple : en « écrivant » sur un mur à l'aide de rafales d'armes au sein d'un jeu de tir (FPS). Ces messages sont quasiment indétectables et disparaissent rapidement.
En ce qui concerne l'enquête sur les attentats de Paris, Une Playstation 4 a été saisie lors des perquisitions en Belgique. Cependant, rien de prouve, à cette heure, que celle-ci ait pu effectivement être utilisée par les auteurs de la manière décrite ci-dessus.

Chiffrement et porte dérobée
D'une manière générale, l'utilisation des outils numériques de communication pose des difficultés techniques et juridiques aux autorités chargées de la surveillance. Depuis l'affaire Snowden et les excès de surveillance de la NSA, les entreprises du secteur (Apple, WhatsApp, etc.) ont renforcé la sécurité de leurs outils pour rassurer leurs clients quant à la confidentialité des données personnelles.
Par exemple, la nouvelle version du logiciel iOS9 pour iPhone et iPad comporte désormais un code de déverrouillage à 6 chiffres au lieu de 4 plus difficile à craquer, y compris la firme Apple elle-même.
De son côté, WhatsApp chiffre les échanges de bout en bout ce qui garantit une totale confidentialité. C'est comme un coffre fort dont on aurait jeté la clé au fond d'un puits…
Dans le cadre de la lutte anti-terroriste, les Etats réclament la possibilité de pouvoir accéder aux communications numériques en bénéficiant des clés de (dé)chiffrement ou via des portes dérobées (backdoors) prévues à l'avance. Mais ces demandes sont en contradiction avec l'exigence de confidentialité des plus farouches partisans de la protection de la vie privée.

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !
Source :
http://www.franceinfo.fr/emission/nouveau-monde/2015-2016/reseaux-sociaux-messageries-jeu-video-comment-les-terroristes-communiquent-16-11-2015-08-49

Le célèbre gestionnaire de mots de passe LastPass hacké

	Le célèbre gestionnaire de mots de passe LastPass hacké

Deux chercheurs ont décortiqué le service en ligne et ont réussi à déchiffrer la base de mots de passe par le biais du processus de récupération de compte.

Diffusé aussi bien auprès du grand public que des entreprises, LastPass est certainement l'un des gestionnaires de mots de passe les plus populaires du moment. Mais est-il réellement sécurisé?
Les hackers Alberto Garcia et Martin Vigo – tous les deux membres de l'équipe sécurité de l'éditeur saleforce.com – ont décortiqué ce service par rétro-ingénierie et viennent de présenter le résultat de leur recherche à l'occasion de la conférence Black Hat Europe 2015. Ils ont trouvé une série de failles qui permettent, dans certains cas précis, d'accéder au Saint Graal : la base de mots de passe.
Dans un premier scénario, ils supposent que l'attaquant a réussi à s'implanter sur l'ordinateur de la personne ciblée, après un première infection. L'une des vulnérabilités présentées par les deux chercheurs – et qui a depuis été patchée – est d'utiliser le processus de récupération de compte. C'est une fonctionnalité fort utile pour les utilisateurs qui ont la mémoire qui flanche, mais qui s'appuie sur un élément fort bizarre: un mot de passe OTP (One Time Password) qui est généré par défaut et stocké en clair sur la machine. En l'intégrant dans une fausse requête de récupération par une requête HTTP, les deux hackers arrivent à ouvrir une session LastPass et à récupérer la version chiffrée de la base de mots de passe.

Un mot de passe boosté aux stéroïdes
Mais ce n'est pas tout: ils reçoivent aussi une version chiffrée de la clé qui permet de déchiffrer la base. Mais le sésame pour déchiffrer cette clé n'est pas très loin: c'est un dérivé de l'OTP par hachage (SHA-256). Bingo, la base est ouverte. Et le mieux dans cette affaire, c'est que cette procédure de récupération court-circuite les protections additionnelles que l'utilisateur peut mettre en place, telles que l'authentification à double facteur ou la restriction d'accès en fonction de l'adresse IP. « D'une certaine manière, l'OTP est un master password boosté aux stéroides », souligne les deux chercheurs, qui ont rapporté leur trouvaille à LastPass.
L'éditeur a, depuis, déployé un correctif qui empêche la création de fausses requêtes de récupération. Par ailleurs, il a introduit il y a quelques semaines un deuxième facteur d'authentification pour valider cette procédure, au travers d'un code envoyé par SMS. Il est vivement recommandé d'activer cette option baptisée « SMS Recovery » dans les paramètres du compte. Les hackers ont également rappelé dans leur présentation qu'il ne fallait jamais cocher la case « Mémoriser le mot de passe » dans le plugin Lastpass. En septembre 2014, ils avaient en effet montré qu'il était possible de le récupérer assez facilement, une fois que l'on a accès à la machine.
Attaque par JavascriptL'autre scénario imaginé par MM. Garcia et Vigo est celui d'un attaquant qui a réussi à accéder aux serveurs de LastPass. Théoriquement, une telle attaque ne devrait pas permettre d'accéder aux mots de passe d'un utilisateur car ils sont stockés de manière chiffrée. Mais les deux chercheurs ont trouvé un moyen détourné. Le service en ligne utilise du code Javascript pour pouvoir renseigner automatiquement les champs d'authentification dans une page web – ce qui est bien pratique.
Exécuté localement sur la machine de l'utilisateur, ce code peut accéder aux identifiants d'un compte en ligne. En insérant son propre code Javascript dans les serveurs de LastPass, un attaquant pourrait alors facilement récupérer ces données secrètes. On peut donc se demander si un tel service est réellement une solution face à des organisations telles que la NSA qui pourraient contraindre l'éditeur à intégrer leur propre code sur leurs serveurs…
Pour autant, pas la peine de jeter le bébé avec l'eau du bain. « LastPass s'est montré très réactif face à ces failles et les a réparé pour la plupart en l'espace de 72 heures », soulignent les chercheurs qui, par ailleurs, continuent à utiliser ce service. Car en dépit des failles potentielles que peut avoir un gestionnaire de mots de passe, ce sera toujours mieux que de noter ses mots de passe dans un tableur !

Source : http://www.01net.com/actualites/black-hat-2015-ils-ont-hacke-lastpass-le-celebre-gestionnaire-de-mots-de-passe-929666.html
Par Gilbert KALLENBORN

Attentats à Paris : les Anonymous promettent une riposte « massive »

Attentats à Paris : les Anonymous promettent une riposte « massive »

Comme après les attentats de Charlie Hebdo en janvier dernier, le collectif Anonymous promet de se venger sur le Web.

Sur une vidéo, un internaute qui se réclame de la nébuleuse de hackers promet une riposte « massive » suite aux attentats qui ont ensanglanté la capitale ce vendredi.

« Ces attentats ne peuvent pas rester impunis. C'est pourquoi les Anonymous du monde entier vont vous traquer. Oui, vous les vermines qui tuent les pauvres innocents, nous allons vous traquer, comme nous avons pu le faire depuis les attentats de 'Charlie Hebdo'. », déclare ce « représentant », caché derrière le fameux masque de V pour Vendetta.

« Attendez-vous donc à une réaction massive d'Anonymous. Sachez que nous vous trouverons et que nous ne lâcherons rien. Nous allons lancer l'opération la plus importante jamais réalisée contre vous, attendez-vous à de très nombreuses cyberattaques. La guerre est déclenchée, préparez-vous. Le peuple français est plus fort que tout et se relèvera de cette atrocité encore plus fort, sachez-le. », peut-on encore entendre.

On se souviendra que les Anonymous ont transmis à Twitter 9.200 comptes liés au groupe Etat islamique et ont lancé l'opération OpCharlieHebdo visant à faire tomber des sites proches de la mouvance islamiste. Des actions qui ont parfois été critiquées par certains observateurs, le risque étant de rendre encore plus discrète la présence en ligne de ces terroristes.

Rappelons que la loi antiterroriste récemment adoptée en France pénalise l'apologie du terrorisme sur Internet et permet un blocage administratif des sites concernés.

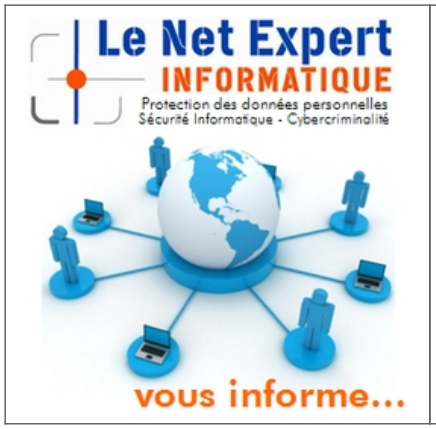
Source :

http://www.zdnet.fr/actualites/attentats-a-paris-les-anonymous-promettent-une-riposte-massive-39828172.htm

---

Les pires et meilleurs endroits pour stocker ses

données | Le Net Expert Informatique



Les pires et meilleurs endroits pour stocker ses données