Attentats : attention au message bidon “On est tous Paris”

Attention au message bidon “On est tous Paris”

Comme après les attentats de janvier, un « hoax » ou « fake » circule à grande vitesse ces dernières heures par SMS, Facebook ou Twitter. Il s'agit d'un message qui dit vouloir prévenir que le mail « On est tous Paris » est dangereux et contient un virus.

En fait, ce message de « prévention » est lui-même potentiellement un virus ou au moins un message bidon qui n'a rien d'officiel.
L'éventuel mail « On est tous Paris » n'existe pas.
Si vous le recevez, soyez vigilants et ne cliquez surtout pas, ne le relayez pas. Il pourrait infecter votre téléphone ou votre ordinateur.
Le voici :

> Vous risquez de recevoir un mail nommé "on est tous Paris" qui est diffusé
> à grande échelle depuis ce WEEK-END.
> Dans ce message une photo de bébé avec un bracelet de naissance où il est
> écrit "on est tous PARIS" vous invitant à cliquer sur la photo.
> Ce message contient un malware (virus) qui permet de prendre le controle à
> distance de votre ordinateur et de récupérer toutes vos données et mots de passe.
> Source : service de cyber criminalité du ministère de la défense.
> Donc, envoyez ce message à vos contacts. C'est urgent et ca va très vite, ca circule depuis dimanche.
> La confirmation de cette info a été diffusée sur EUROPE 1 ce matin.

Ni le service de cybercriminalité du ministère de la défense, ni Europe 1 n'ont diffusé cette pseudo-information. Et les nombreuses fautes d'orthographe et de typographie prouvent facilement que ce message est un « fake ». Ne le diffusez pas !

Depuis vendredi, les rumeurs, fausses infos circulent sur le web. Nous en avons recensé ici :
http://france3-regions.francetvinfo.fr/nord-pas-de-calais/attentats-de-paris-mefiez-vous-des-rumeurs-sur-les-reseaux-sociaux-853751.html

Soyez prudents. Informez sur des sites de confiance et ne relayez pas des images.

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

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !
Source : http://france3-regions.francetvinfo.fr/nord-pas-de-calais/attentats-attention-au-message-bidon-est-tous-paris-855033.html

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

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

---

Après les attentats de Paris, simplification du blocage des

sites Internet terroristes | Le Net Expert Informatique

Après les #attentats de Paris, simplification du blocage des sites Internet terroristes

Le blocage administratif d'un site terroriste veut se passer d'autorité judiciaire? La Cnil y met bon ordre et place un juge au centre de la procédure en désignant Alexandre Linden en tant que personne qualifiée à s'assurer de la régularité d'un blocage.

Selon une information de nos confrères de L'Expansion, confirmée par la suite, la Cnil a nommé Alexandre Linden en tant que « personne qualifiée » pour encadrer le blocage administratif des sites incitant au terrorisme ou en faisant l'apologie. Cette nomination prendra effet dès sa publication au JO. La loi de novembre 2014 fait polémique, du fait notamment qu'une autorité administrative puisse exiger des FAI qu'ils interdisent l'accès à un site sans contrôle a priori d'un juge. Toutefois, cette procédure doit être encadrée par un membre de la Cnil.
L'article 6-1 de la LCEN (modifiée par la loi sur la lutte antiterroriste de novembre 2014) prévoit que la Commission nomme « en son sein » une personne en charge de « s'assurer de la régularité des demandes de retrait et des conditions d'établissement, de mise à jour, de communication et d'utilisation de la liste ». Pour cela, l'autorité administrative (l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication, ou OCLCTIC pour les intimes) doit lui transmettre « sans délai » les demandes de blocage, les listes d'adresses électroniques concernées et les raisons ayant motivé le blocage.

Un juge du blocage sans juge
Cette désignation est loin d'être anecdotique : Alexandre Linden (69 ans) est membre de la Cnil (depuis février 2014), mais aussi et surtout conseiller honoraire à la Cour de Cassation et ancien juge d'instruction. La Commission place donc un ancien magistrat au centre du dispositif de blocage par l'autorité administrative. Laquelle aura dès lors quelques difficultés à contourner le contrôle du juge, puisque celui-ci aura accès aux données relatives aux sites visés et pourra estimer la pertinence d'un blocage.
Toutefois, les recours seront limités, puisque les pouvoirs de cette « personne qualifiée » ne sont pas vraiment terrifiants : « si elle constate une irrégularité, elle peut à tout moment recommander à l'autorité administrative d'y mettre fin ». L'OCLCTIC doit déjà trembler d'effroi… Si jamais l'autorité devait ne pas suivre cet avis, « la personnalité qualifiée peut saisir la juridiction administrative compétente ». Soit faire appel au tribunal administratif et engager une longue procédure, au cours de laquelle le site restera bloqué. On restera donc prudent sur l'efficacité de cette fonction, malgré une nomination hautement symbolique.

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

Source : http://www.linformaticien.com/actualites/id/35731/blocage-administratif-des-sites-la-cnil-nomme-un-juge.aspx

Après les attentats de Paris – Mesures contre le piratage informatique

Après les attentats de Paris – Mesures contre le piratage informatique

Un groupe se réclamant de l'Etat islamique (EI) a piraté, lundi, le compte Twitter du commandement de l'armée américaine au Moyen-Orient et en Asie centrale (US Central Command, CentCom).
Le #ministère français de la Défense a annoncé avoir renforcé ses systèmes de protection contre les attaques informatiques.

Le ministère français de la Défense a annoncé avoir renforcé ses systèmes de protection contre le piratage informatique quelques jours après les attentats jihadistes de Paris et à la suite d'une dizaine d'attaques dont ses sites internet ont été la cible. Deux de ces attaques « concernaient deux régiments de l'armée de Terre, dont une école », a ainsi déclaré à la presse le vice-amiral Arnaud Coustillière, responsable du pôle cyber-défense à l'état-major des Armées.
Au lendemain de la manifestation monstre, dimanche à Paris, en hommage aux 17 personnes tuées dans les attentats de la semaine dernière, « il a été décidé de monter le niveau de vigilance sur internet » et, « depuis mardi, je dispose d'une cellule de crise pour surveiller » les pirates informatiques, a ajouté le vice-amiral Coustillière. « Nous considérons que c'est une crise comme une autre, nous prenons des mesures de précaution et de vigilance (…) mais on ne peut pas parler de cyber-guerre », a-t-il ajouté, rappelant que le ministère de la Défense a environ 350 sites internet.

LE MINISTÈRE DE LA DÉFENSE VISÉ LE 6 JANVIER
« Les attaques contre le site de la Dicod (service de communication du ministère) continuent, il y a régulièrement des gens qui viennent tester le site de la Dicod », a précisé l'officier. « Pour moi, ces attaques sont la réponse à la manifestation de dimanche dernier, par des gens qui n'adhèrent pas à un certain nombre de valeurs », a-t-il dit.
Le site internet du ministère de la Défense avait déjà été cible le 6 janvier d'une attaque informatique revendiquée par le groupe Anonymous qui affirmait vouloir « venger » le militant écologiste Rémi Fraisse tué en octobre pendant la répression d'une manifestation.
Ces données sont à rapporter au fait que, selon les sources ouvertes et disponibles, mais qui n'émanent pas du ministère de la Défense, il y a eu depuis le 10 janvier de l'ordre de 20.000 attaques en France, par des « groupes plus ou moins structurés ou des hackers islamistes bien connus », contre les sites internet les plus variés, d'écoles, d'institutions, de pizzerias, etc., a ajouté le responsable. Ces attaques se font soit par saturation des sites, soit par pénétration ou « défacement », une opération qui consiste à remplacer la page d'accueil par une autre.

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

Source : http://www.parismatch.com/Vivre/High-Tech/Mesures-contre-le-piratage-informatique-691194