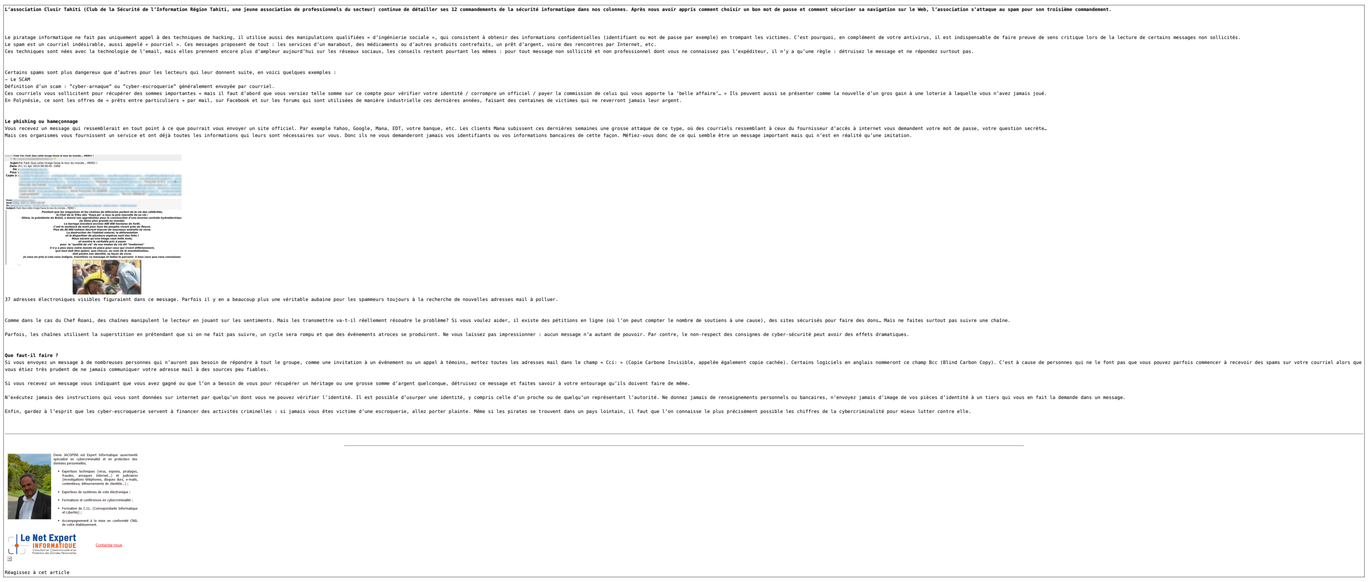
Ne relayez pas les spams, canulars, chaînes de lettres… | Denis JACOPINI

2

	Ne relayez pas les spams, canulars, chaînes de lettres…



L'association Clusir Tahiti (Club de la Sécurité de l'Information Région Tahiti, une jeune association de professionnels du secteur) continue de détailler ses 12 commandements de la sécurité informatique dans nos colonnes. Après nous avoir appris comment choisir un bon mot de passe et comment sécuriser sa navigation sur le Web, l'association s'attaque au spam pour son troisième commandement.

Le piratage informatique ne fait pas uniquement appel à des techniques de hacking, il utilise aussi des manipulations qualifiées « d'ingénierie sociale », qui consistent à obtenir des informations confidentielles (identifiant ou mot de passe par exemple) en trompant les victimes. C'est pourquoi, en complément de votre antivirus, il est indispensable de faire preuve de sens critique lors de la lecture de certains messages non sollicités.
Le spam est un courriel indésirable, aussi appelé « pourriel ». Ces messages proposent de tout : les services d'un marabout, des médicaments ou d'autres produits contrefaits, un prêt d'argent, voire des rencontres par Internet, etc.
Ces techniques sont nées avec la technologie de l'email, mais elles prennent encore plus d'ampleur aujourd'hui sur les réseaux sociaux, les conseils restent pourtant les mêmes : pour tout message non sollicité et non professionnel dont vous ne connaissez pas l'expéditeur, il n'y a qu'une règle : détruisez le message et ne répondez surtout pas.

Certains spams sont plus dangereux que d'autres pour les lecteurs qui leur donnent suite, en voici quelques exemples :
– Le SCAM
Définition d'un scam : "cyber-arnaque" ou "cyber-escroquerie" généralement envoyée par courriel.
Ces courriels vous sollicitent pour récupérer des sommes importantes « mais il faut d'abord que vous versiez telle somme sur ce compte pour vérifier votre identité / corrompre un officiel / payer la commission de celui qui vous apporte la 'belle affaire'… » Ils peuvent aussi se présenter comme la nouvelle d'un gros gain à une loterie à laquelle vous n'avez jamais joué.
En Polynésie, ce sont les offres de « prêts entre particuliers » par mail, sur Facebook et sur les forums qui sont utilisées de manière industrielle ces dernières années, faisant des centaines de victimes qui ne reverront jamais leur argent.

Le phishing ou hameçonnage
Vous recevez un message qui ressemblerait en tout point à ce que pourrait vous envoyer un site officiel. Par exemple Yahoo, Google, Mana, EDT, votre banque, etc. Les clients Mana subissent ces dernières semaines une grosse attaque de ce type, où des courriels ressemblant à ceux du fournisseur d'accès à internet vous demandent votre mot de passe, votre question secrète…
Mais ces organismes vous fournissent un service et ont déjà toutes les informations qui leurs sont nécessaires sur vous. Donc ils ne vous demanderont jamais vos identifiants ou vos informations bancaires de cette façon. Méfiez-vous donc de ce qui semble être un message important mais qui n'est en réalité qu'une imitation.

Sujet : Fw: Fwd: Que cette image fasse le tour du monde... MERCI !
Date : Fri, 11 Apr 2014 09:36:45 -1000
De :
Pour :
Copie à :

Subject: Fwd: Que cette image fasse le tour du monde... MERCI !

Pendant que les magazines et les chaînes de télévision parlent de la vie des célébrités,
le Chef de la Tribu des "Kaya po" a reçu la pire nouvelle de sa vie :
Dilma, la présidente du Brésil, a donné son approbation pour la construction d'une énorme centrale hydroélectrique
(la 3ème plus grande au monde).
Le barrage inondera environ 400 000 hectares de forêt.
C'est la sentence de mort pour tous les peuples vivant près du fleuve,
Plus de 40 000 Indiens devront trouver de nouveaux endroits où vivre.
La destruction de l'habitat naturel, la déforestation
et la disparition de plusieurs espèces sont des faits !
Nous savons qu'une image vaut mille mots,
et montre le véritable prix à payer
pour la "qualité de vie" de nos modes de vie dit "modernes"
Il n'y a plus dans notre monde de place pour ceux qui vivent différemment,
que tout doit être aplani, que chacun, au nom de la mondialisation,
doit perdre son identité, sa façon de vivre.
Je vous en prie si cela vous indigne, transférez ce message et faites-le parvenir à tous ceux que vous connaissez

37 adresses électroniques visibles figuraient dans ce message. Parfois il y en a beaucoup plus une véritable aubaine pour les spammeurs toujours à la recherche de nouvelles adresses mail à polluer.

Comme dans le cas du Chef Roani, des chaînes manipulent le lecteur en jouant sur les sentiments. Mais les transmettre va-t-il réellement résoudre le problème? Si vous voulez aider, il existe des pétitions en ligne (où l'on peut compter le nombre de soutiens à une cause), des sites sécurisés pour faire des dons… Mais ne faites surtout pas suivre une chaîne.

Parfois, les chaînes utilisent la superstition en prétendant que si on ne fait pas suivre, un cycle sera rompu et que des événements atroces se produiront. Ne vous laissez pas impressionner : aucun message n'a autant de pouvoir. Par contre, le non-respect des consignes de cyber-sécurité peut avoir des effets dramatiques.

Que faut-il faire ?
Si vous envoyez un message à de nombreuses personnes qui n'auront pas besoin de répondre à tout le groupe, comme une invitation à un événement ou un appel à témoins, mettez toutes les adresses mail dans le champ « Cci: » (Copie Carbone Invisible, appelée également copie cachée). Certains logiciels en anglais nommeront ce champ Bcc (Blind Carbon Copy). C'est à cause de personnes qui ne le font pas que vous pouvez parfois commencer à recevoir des spams sur votre courriel alors que vous étiez très prudent de ne jamais communiquer votre adresse mail à des sources peu fiables.

Si vous recevez un message vous indiquant que vous avez gagné ou que l'on a besoin de vous pour récupérer un héritage ou une grosse somme d'argent quelconque, détruisez ce message et faites savoir à votre entourage qu'ils doivent faire de même.

N'exécutez jamais des instructions qui vous sont données sur internet par quelqu'un dont vous ne pouvez vérifier l'identité. Il est possible d'usurper une identité, y compris celle d'un proche ou de quelqu'un représentant l'autorité. Ne donnez jamais de renseignements personnels ou bancaires, n'envoyez jamais d'image de vos pièces d'identité à un tiers qui vous en fait la demande dans un message.

Enfin, gardez à l'esprit que les cyber-escroquerie servent à financer des activités criminelles : si jamais vous êtes victime d'une escroquerie, allez porter plainte. Même si les pirates se trouvent dans un pays lointain, il faut que l'on connaisse le plus précisément possible les chiffres de la cybercriminalité pour mieux lutter contre elle.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : http://www.tahiti-infos.com/Clusir-Ne-relayez-pas-les-spams-canulars-chaines-de-lettres_a121624.html

---

Nos ordinateurs ont-ils la mémoire courte ? Vidéo

Nos ordinateurs ont-ils la mémoire courte ? Vidéo

Que trouveront les archéologues du futur, d'ici quelques siècles ou quelques milliers d'années ? Des pierres taillées du paléolithique, des hiéroglyphes, des rouleaux de parchemins probablement, des livres peut-être.

Quelles images, quels sons, quels écrits de notre société restera-t-il dans 2000 ans ? Auront-ils résisté aux épreuves du temps et aux mutations technologiques comme l'ont fait la première photo, le premier film, le premier enregistrement sonore.Mais que deviendront les milliards d'informations engrangées dans les disques durs qui se démagnétisent, et sur les CD ou DVD, qui redoutent la lumière du soleil ?[lire la suite]

LE NET EXPERT

:

• MISE EN CONFORMITÉ RGPD / CNIL

- **AUDIT RGPD ET CARTOGRAPHIE** de vos traitements
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements

• FORMATIONS / SENSIBILISATION :

- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• RECHERCHE DE PREUVES (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• EXPERTISES & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Nos ordinateurs ont-ils la mémoire courte ?*

Les objets connectés représentent-ils un risque ? | Denis JACOPINI

Les #objets connectés représentent-ils un risque ?

Contrôler sa maison ou son appartement du bout des doigts, voici la promesse des fameux objets connectés. Des réfrigérateurs aux téléviseurs, en passant par les thermostats, les caméras de surveillance, les serrures, ou encore les éclairages… de plus en plus d'équipements du foyer peuvent être pilotés à distance à l'aide d'un smartphone via un réseau local et Internet. Mais derrière ce rêve de la maison intelligente et connectée, encore inimaginable il y a quelques années, se cachent d'inquiétants problèmes de sécurité. État des lieux.

Un marché en ébullition

Longtemps réservée aux technophiles fortunés, la domotique commence vraiment à se démocratiser grâce à l'émergence des appareils et objets connectés. Après les équipements multimédias (Smart TV, systèmes Hi-Fi, imprimantes…), les appareils électroménagers connectés – réfrigérateurs, lave-linge, cafetières, réveils, etc.– commencent à débarquer sur le marché. Mais ce sont surtout les systèmes prêts à l'emploi ou les modules adaptables permettant de connecter l'éclairage, les serrures de portes, les stores, les systèmes de surveillance (caméras, détecteurs de mouvements/fumée, alarmes…), ou encore le chauffage qui rencontrent un succès grandissant.
L'embellie du marché de la domotique s'explique notamment par la simplicité d'installation et d'usage de ces nouveaux produits, mais également par leur prix de plus en plus abordable. Toutefois, comme n'importe quel appareil qui se connecte à un réseau Wi-Fi et à Internet, ils s'exposent de fait à toutes sortes de risques. D'autant que pour la plupart, ils ne possèdent aucun système de protection de type antivirus, antimalware, etc. Des failles de sécurité, plus ou moins importantes en fonction de la nature des objets, ont été soit démontrées par des experts de sécurité, soit exploitées par des hackers. Nous verrons les cas les plus effrayants qui donnent matière à réflexion.

Des appareils sous haute surveillance

Outre les incidents révélés ici et là, la sécurité des objets connectés est devenue un sujet particulièrement sensible depuis la médiatisation d'un moteur de recherche public étonnant baptisé Shodan. Créé par un Américain du nom de John Matherly, ce dernier explore le Web en continu pour référencer et regrouper tous les appareils qui y sont connectés. Quelques clics suffisent pour trouver aussi bien des systèmes domotiques, que des imprimantes, des caméras, des alarmes, voire des installations industrielles sensibles telles que des centrales électriques, des raffineries, ou encore, des réacteurs.

Pas de quoi rassurer les utilisateurs, même si à l'origine Shodan n'aurait pas été créé pour nuire, mais au contraire pour aider les experts en sécurité à identifier les vulnérabilités des logiciels et infrastructures réseau des entreprises. Le service se targue de garder une trace de tous les faits et gestes de ses utilisateurs, qui doivent obligatoirement s'identifier et souscrire à un abonnement au-delà d'un certain nombre de recherches. Il n'en reste pas moins que désormais, tout objet connecté ayant une adresse IP peut être localisé, identifié, voire détourné.

Les promesses de la maison intelligente et connectée

Contrôler et gérer divers équipements de la maison à l'aide d'un smartphone, d'une tablette ou d'un ordinateur n'est plus une utopie. Inutile d'avoir à tirer des câbles partout et d'entreprendre de lourds et coûteux travaux avec des spécialistes. Tout le monde peut en principe concevoir une installation domotique soi-même grâce à la nouvelle génération de produits disponibles sur le marché. Au-delà du confort qu'offrent ces nouvelles technologies au quotidien, elles permettent de réaliser de substantielles économies d'énergie, de renforcer la sécurité du foyer, ou encore de se prémunir d'accidents domestiques (incendie, inondation…).

Confort, sécurité, prévention, économie d'énergie…

Domotique

Les produits ont évolué, mais la promesse de la domotique est toujours la même : centraliser et automatiser grâce à diverses technologies l'ensemble ou une partie des équipements électriques du foyer. Des serrures qui se ferment à distance, des caméras et des détecteurs de mouvements capables de s'animer en votre absence et de vous envoyer des SMS en cas d'intrusion, des thermostats intelligents permettant de gérer la température au degré près dans chaque pièce, des stores électriques qui s'ouvrent et se ferment automatiquement en fonction de la lumière, des détecteurs de fumée (obligatoires dans toute l'Union européenne à partir de mars 2015) qui lancent des alertes en cas de départ d'incendie, des éclairages qui créent différentes ambiances lumineuses selon les heures de la journée… Les possibilités sont quasi-infinies.

Réaliser une installation domotique est maintenant à la portée du plus grand nombre grâce, notamment, à ce qu'on appelle les box domotiques. Ces systèmes prêts à l'emploi que l'on trouve dans tous les magasins de bricolage et d'électronique (Castorama, Leroy Merlin, Electro Dépôt…) et même dans certains hypermarchés permettent de connecter et de contrôler à distance des équipements de la maison via une seule et même interface. Ces packs se composent d'un serveur domotique / multimédia (relié au réseau Wi-Fi du foyer), et d'un éventail plus ou moins important d'équipements de surveillance, d'automatisation, de loisirs, etc.

Ces dispositifs communiquent entre eux par le biais de différentes technologies sans fil comme le courant porteur (CPL), le Wi-Fi, les radiofréquences, ou des protocoles propriétaires. Pour les contrôler à l'aide d'une tablette ou d'un smartphone depuis le réseau local du foyer ou à distance par Internet, l'utilisateur n'a plus qu'à jouer du bout des doigts avec les icônes représentant les équipements connectés pour planifier des actions immédiates ou différées.

Créer des scénarios

Dans le jargon de la domotique, un scénario désigne un ensemble d'actions programmées pour différents moments de la journée, de la semaine, du mois, voire de l'année. Les fabricants ont réalisé d'énormes progrès pour faciliter la gestion des produits domotiques et la création de scénarios en développant des applications très intuitives. Exit les lignes de code informatique, ou les menus interminables au vocabulaire incompréhensible, place aux icônes visuelles, aux photomontages représentant les différentes parties du foyer, et à des menus dynamiques inspirés de ceux des smartphones. Quelques clics suffisent pour créer plusieurs scénarios pour la journée, la nuit, le week-end, et les combiner entre eux.

Point d'orgue des maisons intelligentes, les applications mobiles facilitent la compréhension et l'utilisation des équipements domotiques

On peut imaginer, par exemple du lundi au vendredi, un scénario qui consisterait à déclencher une série d'actions à partir de 7 heures : ouvrir les stores, allumer le ballon d'eau chaude, faire chauffer la cafetière, lancer la radio, déverrouiller les portes, démarrer les caméras de surveillance, etc. Bien entendu, toutes les solutions domotiques n'offrent pas les mêmes possibilités. Les fabricants distillent généralement des packs spécialisés dans un domaine précis (surveillance, automatisation, éclairage, chauffage…) à compléter au fur et à mesure. En parallèle, il existe d'innombrables objets connectés autonomes (stations météo, balances Wi-Fi, réveils intelligents, ampoules connectées…) qui se connectent directement au réseau du foyer, sans passer par un serveur propriétaire.

Aura, le réveil intelligent de Withings qui analyse votre sommeil pour vous réveiller en douceur

Le problème, c'est que tout ce petit monde ne parle pas le même langage. Les standards universels, que rêvent de concevoir Apple et Google pour que tous les appareils connectés puissent communiquer entre eux via leurs plateformes mobiles respectives, ne sont pas encore d'actualité. À moins de choisir du matériel très haut de gamme comme la box universelle Lifedomus Vision (2 988 euros) compatible avec la plupart des protocoles de communication des solutions domotiques (KNX, EnOcean, MyHome, Zwave, Modbus, Zigbee…), mieux vaut s'équiper chez le même fabricant pour pallier les éventuels problèmes de compatibilité.

Quels risques pour la sécurité ?

Depuis quelques mois, la sécurité de l'Internet des objets fait couler beaucoup d'encre. Aux quatre coins de la planète, des experts en sécurité prennent le sujet à bras le corps : ils multiplient les démonstrations pour montrer les vulnérabilités de certains produits et la façon dont les cybercriminels pourraient les exploiter pour réaliser des attaques. Les spécialistes n'ont pas tort d'alerter les fabricants, car les risques ne sont plus seulement virtuels. Depuis quelques mois, quelques cas concrets d'attaques basées sur des objets connectés prouvent le bien-fondé de leurs craintes.

Failles et vulnérabilité des objets connectés

La division de sécurité Fortify on Demand du constructeur HP a récemment publié un rapport alarmant sur la sécurité des objets connectés. Elle a ainsi annoncé avoir découvert plus de 25 vulnérabilités sur 10 objets connectés parmi les plus populaires (Smart TV, thermostats intelligents, webcams, boxs domotiques…). Sans donner plus de précisions sur les marques concernées, elle déclare que la plupart ne crypte pas les données échangées sur le réseau et n'exige pas de mot de passe sécurisé mêlant caractères spéciaux et chiffres pour l'accès à distance. Ces dispositifs autorisent des mots de passe comme « 123456 » particulièrement vulnérables (un fait que nous avons effectivement pu vérifier après quelques recherches sur Shodan). Par ailleurs, la protection de leurs logiciels serait insuffisante, car non chiffrée, et certaines interfaces Web ne sont pas du tout sécurisées.

Toujours selon ce rapport, 90 % des produits évalués collectent des informations personnelles sensibles (adresse email/postale, date de naissance…) susceptibles de circuler en clair sur Internet à cause du manque de protection. Difficile néanmoins de contester un rapport ne précisant pas les modèles et les marques des appareils incriminés. À travers cette étude, la division déclare vouloir sensibiliser les acteurs du marché, mais elle souhaite aussi promouvoir sa solution de sécurité Fortify on Demand auprès des fabricants.

Ce n'est pas la seule étude de ce type. Le groupe de chercheurs indépendant d'AV-Test avait mis en lumière d'importantes failles de sécurité, notamment sur les systèmes domotiques iComfort de REVRitter, et XAVAX MAX ! d'Hama, permettant de contrôler le chauffage, l'électricité, les prises de courant avec interrupteur, ou encore l'éclairage. Aussi incroyable que cela puisse paraître, leur communication n'était pas sécurisée sur le réseau lors des mises à jour logicielle ou firmware, mais en plus, la solution iComfort ne nécessitait aucune authentification que cela soit pour l'accès local ou via Internet.

Avec un moteur de recherche comme Shodan, n'importe qui aurait pu repérer les dispositifs de la marque sur Internet et en prendre le contrôle à distance… Effrayant. Gageons que les deux fabricants ont pris les mesures qui s'imposent pour sécuriser un tant soit peu leurs systèmes.

Le lapin Karotz sécurisé ? Pas tout à fait.

Dans la sécurité informatique, les experts réalisent des « exploits », c'est-à-dire des tests (appelés Proof-of-concept, preuve de concept) visant à démontrer la présence de vulnérabilités sur des systèmes ou des logiciels pour proposer des patchs. Certains exemples sont particulièrement croustillants. La spécialiste Jennifer Savage avait ainsi montré comment elle avait réussi à exploiter une faille de sécurité du fameux lapin multifonctions Karotz qu'elle avait offert à sa fille. Cela lui avait permis de prendre le contrôle à distance de l'appareil à son insu, à l'aide d'un ordinateur, et d'utiliser sa caméra et son micro pour l'espionner.

Des ampoules qui éclairent et déverrouillent les réseaux Wi-Fi

Plus récemment, des chercheurs sont parvenus à prendre le contrôle d'ampoules connectées Lifx en exploitant une faille de leur protocole de communication. Ils ont pu démontrer qu'ils pouvaient théoriquement s'introduire dans un rayon de 30 mètres dans le réseau Wi-Fi domestique auquel elles sont connectées et accéder à des données privées stockées sur d'autres appareils du foyer, par exemple. Depuis cette découverte, le fabricant s'est empressé de publier un correctif.

Des Smart TV qui espionnent les téléspectateurs

Les démonstrations les plus impressionnantes ont souvent lieu lors des conférences Black Hat organisées chaque année à Las Vegas, mais aussi à Amsterdam ou à Tokyo. Elles réunissent aussi bien des chercheurs, des experts en sécurité, que des hackers de haut vol. En 2013, plusieurs conférenciers ont exposé les vulnérabilités des TV connectées. L'un d'entre eux a prouvé notamment qu'il était possible de prendre le contrôle de la caméra et du micro d'une Smart TV et d'espionner leur propriétaire à leur insu. Et cela, même quand l'appareil était éteint.

Le thermostat Nest lui qui joue les « Big Brother »

À l'occasion de la dernière édition qui s'est déroulée au mois d'août 2014 à Las Vegas, des chercheurs d'une université de Floride ont montré comment pirater le thermostat intelligent de Nest (la start-up rachetée par Google). Avec un accès physique à l'appareil (uniquement), ils ont pu prouver qu'il est possible d'insérer un code pour détourner et récupérer les informations récoltées par l'appareil, sans que son propriétaire s'en aperçoive.

Nouvelle génération de cyberattaques

La sécurité et la protection des données privées ne sont clairement pas la priorité de certains acteurs du marché des objets connectés. Sans vouloir dresser un tableau catastrophique de la situation, les cyberattaques sur les objets connectés présentant des failles de sécurité ont tendance à se multiplier ces derniers mois. Caméras de vidéosurveillance, réfrigérateurs, babyphones, Smart TV, voici quelques exemples connus d'appareils qui ont fait l'objet d'attaques diverses et variées.

Des caméras au service des voyeurs

Impossible de ne pas citer la faille de sécurité qui avait permis à des hackers de diffuser sur Internet le flux vidéo de milliers de webcams et caméras de vidéosurveillance Trendnet, installées chez des particuliers. Malgré la publication rapide d'un correctif par le fabricant après sa découverte, de nombreux utilisateurs continuaient un an plus tard à être espionnés à leur insu, car ils n'avaient toujours pas fait la mise à jour.

Un hack jusque dans… le berceau d'un nourrisson !

Début 2014, la société spécialisée en sécurité FoolPoint a révélé pour la première fois une cyberattaque réalisée à partir de toutes sortes de dispositifs connectés dont des Smart TV, des NAS, des consoles de jeux vidéo, un réfrigérateur, etc. Les pirates auraient exploité leur vulnérabilité pour installer un serveur de spams (botnet) et envoyer plus de 750 000 emails frauduleux. Dans l'État de l'Ohio aux États-Unis au mois d'avril dernier, un hacker n'a rien trouvé de mieux que de pirater un babyphone pour terroriser un bébé et ses parents. En prenant le contrôle de l'appareil équipé d'une caméra, d'un micro et d'un haut-parleur, il s'est mis à hurler des insanités sur le nourrisson.

Analyse et collecte de données en règle

En Grande-Bretagne, le blogueur spécialisé en développement informatique connu sous le nom de DoctorBeet's a fait une étonnante découverte. Suite à l'acquisition d'une Smart TV de la marque LG, il a remarqué l'apparition de publicités ciblées comme on peut en voir sur des services Web tels que Gmail. Il en a donc déduit que la TV devait forcément analyser ses habitudes, les programmes qu'il regarde, les sites qu'il visite, etc. En cherchant à en savoir plus, il constate en effet que son téléviseur dispose d'une fonction activée par défaut de collecte d'informations de visionnage.

Même après avoir désactivé cette fonction, le téléviseur continuait de transmettre des informations à son insu à LG. Le constructeur ne se contentait pas de scruter ses habitudes de consommation, mais il récupérait également des données personnelles telles que des vidéos de famille qu'il avait projetées sur son écran depuis son ordinateur. Un scandale dont se serait bien passé LG qui aurait, depuis, décidé de permettre à ses clients de « vraiment » désactiver l'option de collecte de données. Outre le manque de sécurité constaté sur de nombreux objets connectés, il faudra donc aussi dorénavant se méfier des pratiques intrusives de certains fabricants !

Source DoctorBeet's Blog

Sous l'œil de Shodan

En faisant un tour d'horizon des objets connectés pour la maison, susceptibles de présenter des risques, on se rend compte qu'ils sont tous potentiellement vulnérables. Certains ne sont pas sécurisés ou pas suffisamment, tandis que d'autres présentent des failles de sécurité plus ou moins importantes pouvant être exploitées pour mener des attaques externes ou à courte distance. Mais la principale faille qu'exploitent les hackers est encore trop souvent l'absence de vigilance des utilisateurs. Beaucoup n'ont pas conscience des risques et n'utilisent pas de mots de passe pour protéger l'accès à distance de leurs équipements, ou se contentent de laisser les identifiants par défaut fournis par les fabricants. Un vrai problème, d'autant qu'avec un moteur de recherche comme Shodan, tous les appareils connectés ayant une adresse IP visible sont désormais répertoriés sur le Web.

D'une efficacité redoutable, ce service permet d'effectuer des recherches globales, ou par pays, en saisissant une simple requête pour identifier, localiser, voire prendre le contrôle des appareils connectés non protégés par un mot de passe. Il suffit de saisir le nom d'une marque de produits connectés connue (DLink, Netgear, Samsung…) ou de cliquer sur les mots recherchés les plus populaires (Webcam, Camera, Netcam…) pour voir apparaître leurs adresses IP et s'y connecter. Le service indique de surcroît de nombreux détails sur les dispositifs, comme leur système d'exploitation, s'ils sont connectés, protégés ou non par des identifiants, etc.

Comme cela avait été démontré dans une enquête baptisée Null CTRL, réalisée par deux journalistes norvégiens pour le site Dagbladet en 2013, d'innombrables équipements connectés référencés par Shodan ne possèdent aucune protection. Quelques clics suffisent pour les repérer et visionner, par exemple, le flux vidéo de caméras de surveillance chez des particuliers, jouer avec le tableau électrique ou le thermostat d'un immeuble, s'introduire dans des bases de données, etc. Gageons qu'à terme, cette surexposition des objets connectés permette de sensibiliser les utilisateurs sur l'importance de sécuriser leur accès.

Qu'en pensent les experts ?

Au-delà des rapports alarmants, des exploits des chercheurs et des affaires relatées dans les médias, nous avons souhaité donner la parole à un expert en sécurité ainsi qu'à un fabricant de solutions domotiques. Tous deux apportent une vision concrète sur les risques que représentent les objets connectés à l'heure actuelle, et donnent quelques conseils aux utilisateurs pour mieux se protéger.

Cybermesures sur les maisons intelligentes

Pour en savoir un peu plus sur les menaces qui planent sur les maisons intelligentes et leurs installations domotiques, nous avons rencontré un expert en sécurité qui travaille depuis plus de dix ans pour Kaspersky Lab Angleterre. Il dresse un portrait plus nuancé que celui des cabinets d'experts en sécurité que nous avons évoqué précédemment.

David Emm

Clubic : Que pouvez-vous nous dire sur la sécurité des objets connectés pour la maison ?

David Emm : Les gens utilisent Internet pour faire des achats, gérer leurs comptes en banque, aller sur les réseaux sociaux mais aussi pour chercher des informations liées à tous les aspects de leur vie quotidienne. Et cela va encore plus loin maintenant que nous utilisons les technologies informatiques pour réaliser des actions qui étaient, par le passé, purement mécaniques, voire manuelles. Malheureusement, lorsque de nouvelles technologies voient le jour, ou lorsque la technologie génère de nouveaux usages, la sécurité n'est souvent pas l'une des priorités. Ce n'est pas un phénomène nouveau et si l'on regarde en arrière, on remarque que les évolutions sont portées par une volonté de simplicité, de réduction des coûts ou d'autres bénéfices, alors que la sécurité n'est envisagée qu'après l'émergence d'un problème. Les risques sont multiples, allant du vol à la manipulation des données. Il est facile d'imaginer par exemple qu'un compteur intelligent soit manipulé pour falsifier la consommation électrique. Pour l'instant, cela reste de l'ordre du possible plus que de celui du réel car à ma connaissance il n'y a eu aucune attaque réelle visant des compteurs électriques.

Clubic : Selon vous, quels sont les types d'appareils domotiques les plus vulnérables ?

David Emm : Lorsqu'ils entendent parler de l'Internet des objets ou de maisons intelligentes, la plupart des gens imaginent leurs appareils traditionnels disposant de nouvelles fonctionnalités (réfrigérateur, contrôle des portes, chauffage central, etc.). Pourtant, ces appareils ne sont pas encore massivement connectés et pour l'instant, leur vulnérabilité a été démontrée le plus souvent au travers d'exploits d'experts dans le cadre de tests. Bien sûr, lorsque ces appareils seront plus courants dans nos vies, je pense qu'ils deviendront régulièrement la cible d'attaques. Mais il faut surtout s'inquiéter de la vulnérabilité d'appareils qui sont aujourd'hui des incontournables, comme par exemples les modems Internet, les tablettes, les smart TV, etc.

Clubic : À quel type d'attaques les maisons intelligentes (Smart Home) sont-elles exposées ?

David Emm : Je dirais qu'il y a trois principales catégories :
1 – Obtenir l'accès à un appareil et l'utiliser pour prendre le contrôle d'autres systèmes connectés dans la maison
2 – Avoir accès à des informations privées ou sensibles, y compris des mots de passe
3 – Falsifier des informations reçues / envoyées par un appareil à l'insu des personnes du foyer

Clubic : Quelles sont les vulnérabilités que vous avez pu constater ?

David Emm : L'un de mes collègues David Jacoby a publié un rapport pour alerter sur les dangers de l'exécution de code à distance et des mots de passe faibles sur les appareils de stockage NAS, mais aussi la possibilité d'orchestrer une attaque de type « man-in-the-middle » (NDRL : l'attaque de « l'homme du milieu » consiste à s'infiltrer sans être vu dans un réseau et y intercepter des informations) via une Smart TV. Il a également découvert des fonctionnalités d'analyses non référencées intégrées dans les routeurs par les constructeurs (sans doute pour des raisons légitimes), mais qui pourraient être exploitées par un attaquant. Un appareil sans fil est repérable et potentiellement vulnérable aux attaques lorsque ses communications ne sont pas cryptées, et que le mot de passe d'accès utilisé est celui par défaut ou faible.

Clubic : Est-ce que Kaspersky envisage de proposer des solutions de sécurité pour les objets connectés ?

David Emm : Ce n'est pas parce qu'il est possible d'installer une solution de sécurité sur les terminaux traditionnels (PC, tablettes, smartphones…), que cela sera possible sur tous les appareils du quotidien qui sont connectés à Internet. Ces appareils pourraient recevoir et envoyer des données sans pour autant autoriser l'installation de code ou disposer de suffisamment d'espace pour le faire. Ils pourraient être vulnérables (par exemple si une Smart TV tourne sous un OS standard, il est possible que le code ne puisse être modifié que par le constructeur). En plus, le vendeur n'est pas toujours le constructeur des composants informatiques intégrés. Cela signifie qu'il pourrait être impossible de patcher ces appareils, même en cas de mise à jour de sécurité disponible via le constructeur des composants. On comprend mieux pourquoi il est primordial que les constructeurs d'appareils et les entreprises qui les exploitent prennent en compte la sécurité dès le début de la fabrication d'un produit. Il est essentiel de pouvoir établir un dialogue entre experts en sécurité et développeurs d'appareils informatiques pour maisons connectées.

Clubic : Que peuvent faire les utilisateurs pour protéger au mieux leurs systèmes domotiques ?

David Emm : La première chose est de lister tous les objets connectés de la maison et de savoir comment et à quoi ils sont connectés (à Internet, ou à d'autres objets de la maison). Ensuite, il est impératif de mettre des obstacles sur la route du hacker. Pour ce faire, il faut tout d'abord installer régulièrement les mises à jour de sécurité et les mises à jour logicielles, pour limiter le nombre de vulnérabilités connues qui pourraient être exploitées. Après, il faut changer le nom et le mot de passe par défaut de chaque objet connecté, car c'est la première chose qu'un hacker tentera d'attaquer pour en prendre le contrôle. Pour finir, il faut limiter l'accès d'un objet connecté aux autres objets connectés dans la maison. Par exemple, si vous avez une Smart TV, vous devrez restreindre l'accès à cette TV et autoriser seulement son accès à des ressources particulières du réseau (il n'est pas vraiment nécessaire que votre imprimante soit connectée à votre TV, par exemple…).

Clubic : Selon vous, quel serait LE scénario catastrophe pour une maison intelligente ?

David Emm : C'est une question difficile, car LE scénario catastrophe impliquant un seul individu n'aura pas forcément le même impact au niveau d'une communauté. Pour les individus, le risque qui importe c'est le #vol de données personnelles – par exemple, les noms d'utilisateurs, les mots de passe, etc. Ou encore, le fait que l'on puisse vous espionner vous ou votre famille (comme le hack du babyphone survenu dans l'Etat de Ohio). Il y aussi le risque qu'une application contrôlant la sécurité de votre porte d'entrée puisse être hackée, vous laissant enfermé dehors. Du point de vue de la communauté, l'impact peut être plus important. Si un hacker arrive par exemple à intercepter des données d'un compteur intelligent (Smart Meter), cela peut affecter les relevés : il peut remettre les compteurs à zéro, voire créer une panne générale d'électricité.

Le point de vue d'un spécialiste de la domotique

Pour compléter ce dossier, nous avons voulu donner également la parole à un fabricant de solutions domotiques. Somfy, l'un des leaders du marché de la domotique, a bien voulu répondre à nos questions sur la sécurité des maisons intelligentes.

Clubic : Comment la box Somfy et les appareils qu'elle permet de piloter à distance sont-ils protégés ?

Somfy : En tant que spécialiste de solutions domotiques, notre box prend en compte les problématiques de sécurité. L'ensemble des actions effectuées avec nos solutions Tahoma et Somfy Box transite sur un serveur sécurisé et est chiffré sur 128 bits. Le protocole RTS propriétaire de Somfy (10 millions de systèmes installés dans le monde) qui est utilisé pour la commande radio est sécurisé grâce à un code tournant de 16 millions de combinaisons.

Clubic : En tant que fabricant, que pensez-vous du remous médiatique autour de la vulnérabilité supposée ou avérée de certains objets connectés pour la maison ?

Somfy : Nous sommes aujourd'hui en plein boom des objets connectés, avec de nombreux nouveaux acteurs qui lancent parfois des solutions un peu trop vite et pas suffisamment abouties. Il faut veiller à bien se renseigner sur le fabricant et sa légitimité sur le secteur. Somfy possède une expertise en matière de radio et d'IP qui nous rend légitimes sur ce secteur. Depuis que nous avons lancé notre box il y a quatre ans, aucun piratage ne nous a été signalé.

Clubic : Quels sont selon vous les points faibles d'une installation, ou quels pourraient-ils être ?

Somfy : Les points faibles de l'installation seraient de ne pas avoir de système de protection, d'avoir positionné les détecteurs de mouvements aux mauvais endroits ou de ne pas couvrir tous les accès de la maison.

Clubic : Selon vous, quel serait LE scénario catastrophe pour une maison intelligente ?

Somfy : Le scénario catastrophe, s'il y en a un, serait de se faire voler son téléphone sans code pour le déverrouiller en laissant ainsi libre accès à l'application qui commande la maison intelligente. Il faut donc prendre les précautions nécessaires.

Conclusion

En moins de deux ans, la domotique est passée d'un marché de niche à un nouvel eldorado convoité par la plupart des géants de l'industrie high-tech. Apple, Google, Microsoft ou encore Samsung, pour ne citer qu'eux, se sont lancés tour à tour sur ce marché promis à une très forte croissance en multipliant les partenariats et les rachats de start-up spécialisées. Début 2014, Google n'a pas hésité par exemple à faire la troisième acquisition la plus importante de son histoire, en rachetant Nest Labs pour la bagatelle de 3,2 milliards de dollars et, plus récemment, le spécialiste de caméras IP Dropcam pour 555 millions de dollars.

Courant 2014, Samsung s'est offert la start-up spécialisée SmartThings (montant de l'achat non divulgué), Microsoft a noué un partenariat avec Insteon, un des leaders de la domotique aux USA, et Apple a dévoilé à l'occasion de la WWDC la plateforme HomeKit pour iOS8 qui permettra de contrôler les objets connectés de nombreux fabricants via Siri (l'assistant vocal d'Apple). En attendant les solutions des poids lourds des nouvelles technologies, le marché est déjà bien occupé par les acteurs historiques – Somfy, Philips, Haier, Legrand, etc. –, une foule de nouveaux fabricants de tous horizons, des fournisseurs d'électricité ou encore des opérateurs comme Orange et SFR, qui commercialisent en France des kits de domotique pour accompagner leurs box. Si tout ce monde frappe à la porte de nos foyers, c'est que le potentiel est énorme.

Il ne fait aucun doute que les produits du quotidien vont être de plus en plus connectés (comme nous avons pu le voir au CES cette année), mais pas toujours bien sécurisés. Les acteurs comme Google, Apple et Microsoft, qui ambitionnent qu'un maximum d'objets connectés puissent fonctionner à l'avenir avec leurs plateformes mobiles respectives, vont sans doute imposer aux fabricants un cahier des charges drastique en matière de sécurité s'ils veulent obtenir une certification. Cela pourrait peut-être permettre d'augmenter le niveau de protection des objets connectés, même si comme nous l'avons vu, il n'est pas toujours possible de patcher des produits comprenant des composants provenant de différents fabricants.

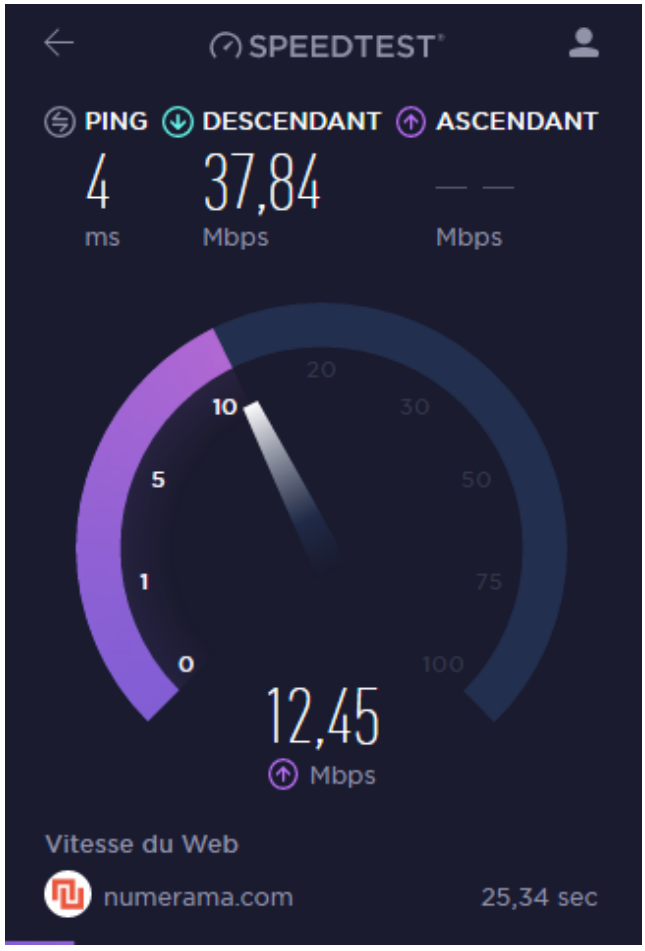
Le nombre croissant d'objets connectés risque d'intéresser de plus en plus les cybercriminels pour entreprendre des diffusions de spams ou de logiciels malveillants à grande échelle, par exemple. Mais le plus effrayant serait qu'ils puissent prendre le contrôle total des maisons intelligentes, espionner leurs habitants à l'aide des caméras de surveillance, s'introduire ni vu ni connu dans le foyer en déverrouillant la porte à l'aide d'un smartphone, couper l'électricité ou le chauffage en plein hiver, ou encore, déclencher l'alarme au beau milieu de la nuit…

Pour que les maisons intelligentes tiennent vraiment toutes leurs promesses, il est indispensable qu'à l'avenir leur sécurité soit garantie. En attendant, côté utilisateur, il faudra être de plus en plus vigilant, se renseigner sur le système de protection des produits, faire systématiquement les mises à jour, ou encore instaurer un mot de passe fort pour l'accès à distance de tous les appareils connectés. Le prix à payer pour que le rêve de posséder une maison intelligente ne tourne pas au cauchemar.

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

Source : #http://www.clubic.com/antivirus-securite-informatique/article-723729-1-objets-connectes-representent-risque.html
Par Jérôme Cartegini

Comment mesurer et tester le débit de votre connexion internet | Denis JACOPINI



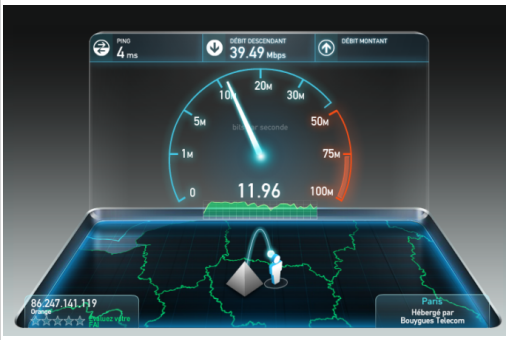
Comment mesurer et tester le débit de votre connexion internet

Internet c'est bien. Quand c'est rapide, c'est mieux. Nous vous avons listé quelques outils indispensables pour mesurer votre débit, que vous soyez chez Free, SFR, Orange, Numericable ou Bouygues.

On entend souvent dire qu'aujourd'hui on ne peut plus vivre sans Internet. Cette affirmation est fausse. Dire qu'on ne peut plus vivre sans **bonne** connexion Internet serait plus juste. Et justement, pour connaître la qualité de votre bande passante, il existe quelques outils extrêmement simple d'utilisation. Petit tour d'horizon des indispensables pour ceux qui ne les connaîtraient pas.

SPEEDTEST

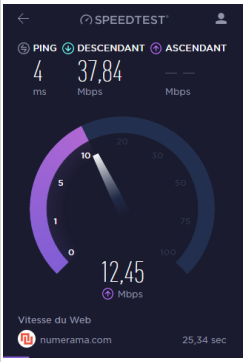
C'est le plus connu des outils présentés ici. Speedtest est complet et calcule votre débit montant et descendant ainsi que le temps de latence. Vous avez ainsi en main absolument toutes les informations en main pour connaître la vitesse de votre connexion. On regrette seulement le temps assez long que peut prendre un test (environ 47 secondes) et l'interface qui manque de sobriété.



Cela devrait bientôt changer grâce à la version HTML5 – encore en version beta – plus simple et efficace. Attention, celle-ci ne fonctionne pas lorsque le bloqueur de publicité est activé. Speedtest se décline également en application mobile pour profiter des mêmes fonctionnalités sur son smartphone.

EXTENSION OOKLA

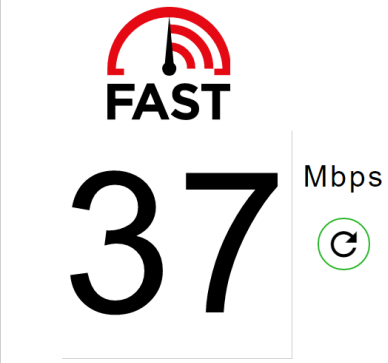
Cet outil est extrêmement pratique. Ookla, l'entreprise qui a créé Speedtest, a sorti une extension Chrome rapide et ergonomique. À l'instar du site Internet, elle calcule le download, l'upload et le ping. Le test est réalisé en un peu moins de 30 secondes mais c'est surtout par son extrême simplicité d'utilisation que l'extension séduit.



En effet, pas besoin de taper l'adresse d'un site ou de lancer une recherche Google. Un simple clic en haut à droite de votre navigateur suffit à y accéder. Ainsi, si vous remarquez certaines lenteurs de connexion, pas besoin d'attendre une éternité avant d'accéder à la page qui pourra vous confirmer que votre débit est pourri. Vous pouvez d'ailleurs fermer la fenêtre de l'extension, celle-ci continuera à faire le test de débit discrètement.
Malheureusement pour tous ceux qui n'utilisent pas le navigateur web de Google, l'add-on Ookla est disponible uniquement sur Chrome.

FAST.COM

En moins de dix secondes, Fast.com calcule votre vitesse de téléchargement (débit descendant uniquement). Si vous n'en avez rien à faire du temps de latence ou que vous n'avez rien à uploader, il s'agit du site idéal.



Ce site est en accord avec la vision de Netflix, son créateur, qui s'adresse plus aux internautes qui consomment plutôt qu'à ceux qui produisent. Ainsi, si vous ne surfez sur le web que pour consulter et télécharger des fichiers, Fast.com représente la meilleure solution. Le service en HTML 5 fonctionne aussi bien sur PC que sur mobiles, smart TV ou tablettes.
Article original de Omar Belkaab

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Guide : comment mesurer et tester le débit de sa connexion internet – Tech – Numerama

---

Attention, l’employeur peut lire les SMS des téléphones professionnels | Denis JACOPINI

23

Une décision de la Cour de cassation permet désormais à une entreprise de lire les messages reçus et envoyés sur un téléphone professionnel. Comme elle pouvait déjà le faire avec les e-mails.
Gare aux sanctions si vous refusez l'accès à vos SMS à votre employeur.

Appelée à statuer sur le litige opposant deux sociétés de courtage, la Cour de cassation a pris une décision qui va concerner des centaines de milliers de salariés : elle a validé le principe selon lequel les SMS envoyés ou reçus par un téléphone mis à la disposition par une entreprise sont « présumés avoir un caractère professionnel ». Par conséquent, les employeurs sont autorisés à lire ces messages, même hors de la présence des salariés.
« Cet arrêt est dans la droite ligne de décisions prises depuis quelques années, nous explique Olivier Iteanu, avocat à la cour d'appel de Paris. Peu à peu la jurisprudence en vient à plus protéger l'entreprise que le salarié. »
L'avocat rappelle ainsi qu'en 2012, un employeur avait été autorisé à consulter le contenu de la clé USB d'un salarié car celui-ci l'avait branchée sur le système informatique de l'entreprise. Un an plus tard, la Cour de cassation confirmait que les employeurs pouvaient consulter les e-mails de la boîte professionnelle de leurs salariés, même hors de leur présence, s'ils n'étaient pas identifiés comme personnels.
Concrètement, grâce à la décision prise en ce mois de février 2015, un employeur ayant « un motif légitime » peut vérifier les SMS en prenant le téléphone de son salarié ou « placer, en passant par des outils de Mobile Device Management (gestion de terminaux mobiles), des logiciels qui vont monitorer ce qui se passe sur le smartphone, pour en extraire les SMS qui pourront être analysés », nous précise Jean Pujol, manager au sein de l'entité conseil en stratégie SI du cabinet Kurt Salmon. « Les SMS peuvent aussi être stockés sur des serveurs centraux, comme cela était le cas dans l'affaire jugée par la Cour de cassation. »

Refuser le contrôle entraînera une sanction
Pour Me Martine Ricouart-Maillet, vice-présidente de l'Association française des correspondants à la protection des données personnelles et associée au sein du cabinet BRM Avocats, « afin d'éviter tout litige, le salarié doit être informé de l'usage qu'il peut faire des outils mis à sa disposition dans la charte informatique de l'entreprise. Cette charte doit aussi l'avertir des moyens de surveillance dont dispose son employeur. »
« Et s'il refuse de se soumettre à ce contrôle, ajoute Me Iteanu, le salarié pourra être sanctionné. » La sanction « suprême » étant le licenciement. Pour lui, cette décision risque d'induire des comportements abusifs de la part de certains employeurs. « Les juges devront très probablement se saisir de cas pour rétablir l'équilibre entre les parties », estime-t-il.
La seule solution pour protéger certains SMS est de les identifier comme personnels. Même si cela n'interdit pas à l'employeur de les lire, cela l'empêche de les utiliser contre un employé. Autre méthode, plus radicale : disposer de deux appareils, un professionnel et un personnel.

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

Source : http://www.01net.com/editorial/646337/attention-votre-employeur-va-pouvoir-lire-les-sms-de-votre-telephone-pro/
Par Cécile Bolesse

Piratage de ses comptes sociaux : prévenir, repérer

et réagir | Denis JACOPINI

Piratage de ses comptes sociaux : prévenir, repérer et réagir !

Sur les réseaux sociaux, la plus grande vigilance est requise si l'on veut protéger ses données personnelles.

Les réseaux sociaux se multipliant de façon considérable, il convient de se montrer attentif à la protection des données personnelles, car ces dernières peuvent d'autant plus facilement être piratées.
A ce titre, la Commission nationale de l'informatique et des libertés (CNIL) publie une fiche pratique, agrémentée de liens directs vers les principaux réseaux sociaux, afin de mettre en oeuvre le contrôle des données personnelles.

Parmi les conseils donnés par la Commission, citons :
– le choix de mots de passe complexes, mais aussi différents les uns des autres, et avec un sens n'ayant aucun rapport avec une donnée personnelle relative à la vie privée du titulaire du compte (comme une date de naissance, etc…) ;
– l'absence totale de communication du mot de passe à une tierce personne ;
– l'activation d'un dispositif d'alerte en cas d'intrusion (dans ce cas, la personne titulaire du compte et qui se connecte depuis un poste informatique inconnu doit confirmer l'accès en entrant un code, reçu préalablement par sms ou par mail) ;
– la déconnexion à distance des terminaux encore liés au compte ;
– la désactivation des applications tierces encore connectées au compte ;
– le réglage précis des paramètres de confidentialité.
En outre, la CNIL donne des astuces pour repérer le piratage d'un compte. Des signes doivent en effet alerter l'utilisateur, par exemple un mot de passe invalide, ou des comportements inhabituels ayant lieu sur le compte, sans consentement préalable (comme suivre, se désabonner, ou encore bloquer…).

En cas de piratage, il convient donc :
– en premier lieu, de signaler le compte piraté auprès du réseau social ;
– cette première étape franchie, il convient alors de demander une réinitialisation du mot de passe. Si la réponse apportées par les modérateurs du réseau n'est pas satisfaisante, la CNIL peut être saisie.

Consultez la fiche pratique de la CNIL

Source : http://www.net-iris.fr/veille-juridique/actualite/34642/comment-prevenir-le-piratage-de-son-compte-en-ligne.php

10 conseils pour garder vos appareils protégés pendant les vacances | Denis JACOPINI

10 conseils pour garder vos appareils protégés pendant les vacances

Si vous faites partie de ces vacanciers qui ne partent jamais sans leurs objets connectés, voici un mini-guide conçu par les experts ESET pour voyager et surfer en toute tranquillité.
Brosse à dents ? ok.
Serviette de bain ? ok.
Ordinateur, téléphone, tablette ? ok.
Si vous faites partie de ces vacanciers qui ne partent jamais sans leurs objets connectés, méfiez-vous des menaces lorsque vous utilisez un Wi-Fi public pour vous connecter à votre banque en ligne, boutique en ligne ou tout simplement pour vérifier vos e-mails. Pas de panique ! Stephen Cobb et d'autres professionnels ESET ont créé un guide pour vous permettre de voyager en toute sécurité et garder ainsi toutes vos données personnelles et vos appareils protégés.

Conseils

1. Avant de prendre la route, assurez-vous d'exécuter sur vos appareils une mise à jour complète du système d'exploitation ainsi que des logiciels, et de posséder une solution de sécurité de confiance.
2. Sauvegardez vos données et placez-les dans un endroit sûr. Pensez à déplacer les données sensibles du disque dur de votre ordinateur portable sur un disque dur externe chiffré le temps de vos vacances.
3. Ne laissez jamais vos appareils sans surveillance dans les lieux publics. Activez la fonction antivol de vos appareils pour tracer les appareils volés ou perdus, et au besoin d'effacer les contenus à distance.
4. Mettez un mot de passe fort et activez la fonction « délai d'inactivité » sur tous vos appareils, que ce soit votre ordinateur portable, votre tablette ou votre téléphone. Retrouvez tous nos conseils pour un mot de passe efficace en cliquant ici.
5. Dans la mesure du possible, utilisez uniquement des accès internet de confiance. Demandez à votre hôtel ou l'endroit où vous logez le nom de leur Wi-Fi et utilisez exactement le même nom : faites attention aux arnaques qui essaient de ressembler aux Wi-Fi publics en ajoutant le mot « gratuit » au nom de la connexion Wi-Fi.
6. Si l'Internet de votre hôtel vous demande de mettre à jour un logiciel afin de pouvoir vous connecter, déconnectez-vous immédiatement et informez-en la réception.
7. Ne vous connectez pas à des connexions Wi-Fi qui ne sont pas chiffrées avec WPA2. Toutes les normes inférieures à celle-ci ne sont tout simplement pas assez sûres et peuvent être facilement piratées.
8. Si vous devez utiliser le Wi-Fi public pour vous connecter à votre réseau d'entreprise, utilisez toujours votre VPN (réseau virtuel privé).
9. Si ce n'est pas urgent, évitez les banques et boutiques en ligne quand vous utilisez le Wi-Fi public. Sinon, nous vous conseillons d'utiliser le partage de connexion de votre téléphone et de surfer en utilisant internet sur votre téléphone portable.
10. Si vous n'utilisez pas encore d'antivirus de confiance et suspectez votre ordinateur portable d'être infecté, vous pouvez utiliser gratuitement le scanner ESET Online qui ne nécessite aucune installation et peut être utilisé pour détecter et retirer des logiciels malveillants
Article original de ESET
Cliquez ici

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Liberté) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : ESET — Actualités

Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits | Denis JACOPINI

Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits

Ce sont les vacances mais nombre de touristes ne se séparent pas de leurs smartphones, tablettes ou ordinateurs portables. Et pour se connecter à l'internet, quoi de mieux qu'attraper un wi-fi gratuit. Une pratique qui peut se révéler très dangereuse. Des proies faciles pour les « sniffeurs » de données. Explications de Laurent Heslault, expert sécurité chez Symantec.

Vous êtes sur votre lieu de vacances et vous avez envie de vous connecter à l'internet. Pour consulter votre messagerie ou vos réseaux sociaux, envoyer des photos à vos proches, surfer sur le net ou consulter votre compte en banque ou faire une réservation.
Solution la plus simple : se connecter à un réseau Wi-Fi gratuit. Dans votre hôtel, camping, à la terrasse d'un café ou d'un restaurant… Les accès gratuits pullulent et se généralisent.
Expert en sécurité à Symantec, Laurent Heslault tire le signal d'alarme. « **Rien de plus simple que de pirater les données qui transitent sur un réseau Wi-Fi gratuit** » assure-t-il. « **Par exemple, je m'installe à la terrasse d'un café et je crée un vrai faux point d'accès gratuit en empruntant le nom du café. Des gens vont s'y connecter et je n'ai plus qu'à récupérer toutes les données qui m'intéressent. Des mots de passe, des identifiants…** »

Des sniffeurs de données

Il exagère ? Non. « **L'expérience a été faite à la terrasse d'un café. Nous avons installé un logiciel qui permet de sniffer tous les appareils qui se branchaient sur le Wi-Fi. Ensuite, des complices, qui se faisaient passer pour des magiciens, allaient voir les gens en disant que par magie, ils avaient réussi à changer le code de leur téléphone ou leur image sur Facebook. Ils étaient étonnés !** » Rien de magique mais des logiciels de piratage qui se trouvent facilement sur le net.

Les données sur le Wi-Fi ne sont pas chiffrées

« **Les données qui transitent sur le Wi-Fi ne sont pas chiffrées. Sauf quand vous vous connectés à un site sécurisé avec le protocole HTTPS. Donc ce sont des données faciles à intercepter.** » Danger sur les vrais faux points d'accès Wi-Fi mais aussi sur les vrais qui ne sont, dans la grande majorité des cas, pas chiffrés non plus. « **Par contre pas de problème pour une connexion 3G ou 4G qui sont chiffrées. Mais pour économiser leur forfait, les gens préfèrent se connecter au Wi-Fi** ».

Conseils

Alors quels conseils ? « **Ne jamais, sur un Wi-Fi public, entrer un mot de passe. D'autant que la plupart des internautes utilisent le même mot de passe pour tous leurs sites.** » En clair, limiter les dégâts en ne consultant que des sites qui ne demandent aucune identification.
Autre solution : protéger son smartphone ou sa tablette en y installent un logiciel qui va chiffrer toutes les données qui vont en sortir. Plusieurs types de logiciels existent dont le Wi-Fi Privacy de Norton qui est gratuit pendant 7 jours et peut s'installer sur des périphériques fonctionnant sous Ios et Androïd.
Article original de Samuel NOHRA.

Nous prodiguons une multitude d'autres conseils durant les formations que nous animons à destination des élus, chef d'entreprises, agents publics et salariés. [Consultez la liste de nos formations]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits

Mise en conformité RGPD : Accompagnement personnalisé par des Experts

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

LE NET EXPERT AUDITS & EXPERTISES | EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES LENETEXPERT.fr | RGPD CYBER . LE NET EXPERT MISES EN CONFORMITÉ | SPY DETECTION Services de détection de logiciels espions | LE NET EXPERT FORMATIONS | LE NET EXPERT ARNAQUES & PIRATAGES

Mise en conformité RGPD : Accompagnement personnalisé par des Experts

Nous semblez manifester un intérêt pour le RGPD (peut-être un peu par obligation) et vous souhaitez nous faire part d'un projet. Nous vous remercions pour votre confiance.
Intervenant sur des missions RGPD depuis 2012, après avoir identifié différents types d'attentes, nous avons adapté nos offres pour qu'elles correspondent au mieux à vos besoins.
Ainsi, nous pouvons vous accompagner dans la mise en conformité de votre structure de plusieurs manières :

1. **Vous recherchez l'autonomie ?**

Nous pouvons vous accompagner pour apprendre l'essentiel de la réglementation Européenne relative à la Protection des Données à Caractère Personnel et le nécessaire pour comprendre et démarrer une mise en conformité. Une fois la formation achevée, vous êtes autonome mais pourrez toujours compter sur notre soutien soit sous forme de formation personnalisée, soit sous forme d'accompagnement personnalisés ;
A l'issue de cette formation, nous vous remettons une attestation prouvant la mise en place d'une démarche de mise en conformité de votre établissement avec le RGPD (Règlement Général sur la Protection des Données). Pour information, nous sommes référencés auprès de la CNIL.

2. **Vous souhaitez être accompagné pour la mise en place de la mise en conformité ?**

Nous réalisons pour vous l'audit qui mettra en exergue les points à améliorer. Au terme de cette étape vous pourrez, si vous le souhaitez, réaliser la mise en conformité ou nous laisser procéder aux améliorations que vous aurez validées ;
A l'issue de cet audit, nous vous remettons un compte rendu prouvant la mise en place de corrections dans le cadre de votre démarche de mise en conformité de votre établissement avec le RGPD (Règlement Général sur la Protection des Données).

3. **Vous souhaitez confier la totalité de votre mise en conformité ?**

De manière parfaitement complémentaire avec votre prestataire informatique et éventuellement avec votre service juridique, nous pouvons vous charger de la totalité de la démarche de mise en conformité de votre établissement avec le RGPD (Règlement Général sur la Protection des Données) et les différentes réglementations relatives à la protection des Données à Caractère Personnel.
De l'audit au suivi, vous pourrez compter sur notre expertise à la fois technique et pédagogique pour que votre établissement soit accompagné de manière externalisée.

Afin de vous envoyer une proposition personnalisée adaptée à la fois aux besoins de votre structure, conforme à votre stratégie et à vos priorités, vous souhaiteriez que vous répondiez à ces quelques questions :

Nous vous garantissons une confidentialité extrême sur les informations communiquées. Les personnes habilitées à les consulter sont soumises au secret professionnel.

Votre Prénom / NOM (obligatoire)

Société / Organisme

Votre adresse de messagerie (obligatoire)

Un numéro de téléphone (ne sera pas utilisé pour le démarchage)

Pouvez-vous nous décrire brièvement votre activité ? (obligatoire)

Remarque :
Vous pouvez nous écrire directement un message dans la zone « INFORMATIONS COMPLÉMENTAIRES QUE VOUS JUGEZ UTILES ». Néanmoins, si vous souhaitez que nous vous établissions un chiffrage précis, nous aurons besoin dans un premier temps des informations ci-dessous.

POUR VOTRE MISE EN CONFORMITÉ RGPD :

1. La découverte de vos obligations : Souhaitez-vous découvrir le RGPD et l'essentiel pour comprendre et démarrer la démarche ? (recommandé)	○Oui○Non
2. Concernant l'Audit : Il consiste à relever les éléments permettant de constituer un état des lieux précis puis à réaliser l'analyse réglementaire du contexte de départ. Nous considérons qu'au moins une journée dans vos locaux est indispensable. La suite de la démarche peut être faite à distance.	Sélectionnez votre choix
3. Concernant la mise en conformité : Elle consiste à mettre en place des améliorations :	Sélectionnez votre choix
4. Concernant le suivi de la mise en conformité : Cette phase consiste à maintenir la mise en conformité avec le temps par une mise à jour précise du registre des traitements./sst-	Sélectionnez votre choix
5. Votre demande concerne-t-elle un groupement de professionnels ? (corporation, fédération, à nous préciser dans les commentaires...) ou est-elle formulée à titre individuel ?	○Groupement○Individuel

INFORMATIONS COMPLÉMENTAIRES QUE VOUS JUGEZ UTILES :

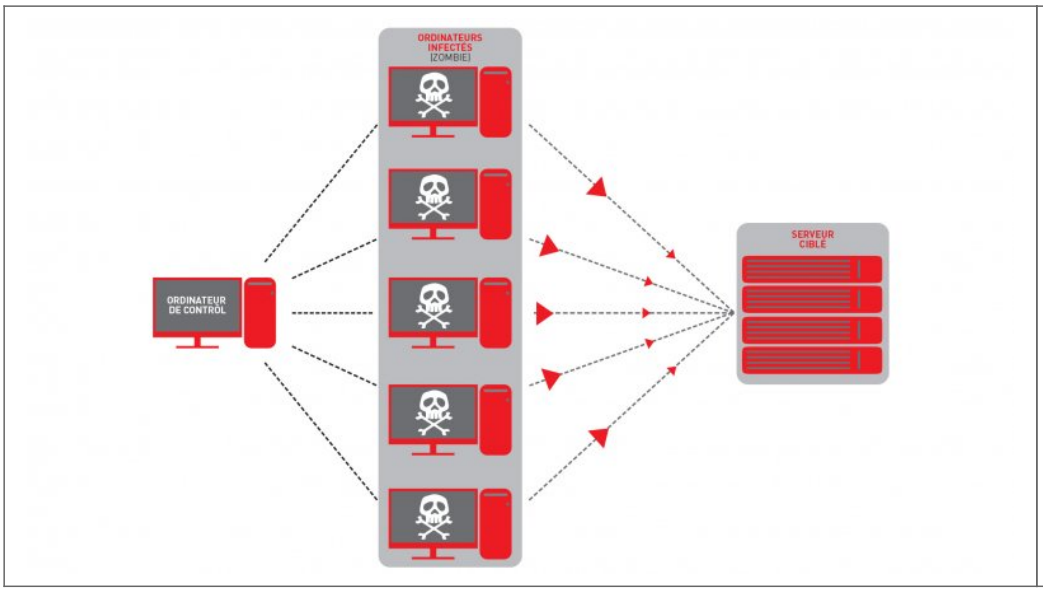
Envoyer
block id="24886" title="Mentions légales formulaires"]

ou bien, envoyer un e-mail à rgpd[a-ro-ba-se]lanetexpert.fr

Denis JACOPINI est notre Expert qui vous accompagnera dans votre mise en conformité avec le RGPD

Je me présente : Denis JACOPINI. Je suis Expert en informatique assermenté et **spécialisé en RGPD (protection des Données à Caractère Personnel) et en cybercriminalité**. Consultant depuis 1996 et formateur depuis 1988, j'ai une expérience depuis 2012 dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données (DPO n°15045), en tant que praticien de la mise en conformité et formateur, je vous accompagne dans toutes vos démarches de mise en conformité avec le RGPD.
« Mon objectif est de mettre à disposition toute mon expérience pour mettre en conformité votre établissement avec le RGPD. »

Qu’est-ce qu’une attaques DDOS et comment s’en protéger ? | Denis JACOPINI



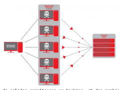
Qu’est-ce qu’une attaques DDOS et comment s’en protéger ?

Suite aux récentes attaques du PSN et du XBL, il nous semblait important d'approfondir le sujet, et de tenter d'expliquer ce qu'est le DDOS. Dans cette optique nous allons essayer d'être le plus précis possible pour comprendre les tenants et les aboutissants de cette méthode. Mais que ce soit clair, nous ne vous apprendrons pas à lancer une attaque de ce genre.

QU'EST-CE QU'UNE #ATTAQUE DDOS ?
Une attaque de ce type a pour but de faire tomber un ou plusieurs serveurs, en envoyant une tonne de requêtes de connexion. Pour faire simple, faisons un parallèle : Imaginons que le serveur soit un évier qui laisse couler un certain volume d'eau. Ici, le DDOS aurait pour effet de rajouter des robinets supplémentaires, jusqu'à ce que l'évier déborde.
En informatique c'est la même chose. Le pirate par le biais de ses « zombies » (nous en parlerons dans le chapitre suivant) envoie des requêtes en continu, sur plusieurs heures voire plusieurs jours jusqu'à ce que le serveur sature et ne puisse plus accepter de requêtes de connexion. Les conséquences sont l'arrêt pur et simple du ou des serveurs, ce qui obligera le prestataire à les purger pour les remettre en fonction (pour reprendre le parallèle de l'évier, on ferme la vanne principale et on vide le bac en totalité).

une attaque de très grande ampleur peut envoyer des requêtes de plusieurs terabytes
Il faut aussi comprendre qu'une attaque de très grande ampleur peut envoyer des requêtes de plusieurs terabytes, de manière continue pendant des jours. Ce qui met très largement à mal les serveurs aussi gros soient-ils et ce même si ils sont dotés d'un système anti DDOS.

EN DDOS, ON PARLE DE ZOMBIE
Le principe même du DDOS, même si il paraît simpliste pour la majorité d'entre vous, est plus complexe qu'il n'y paraît. Dans la pratique, il faut un certain niveau de connaissance pour lancer une attaque d'une certaine ampleur. Oui, il est facile d'attaquer un serveur tout seul via un des logiciels prévus pour, mais l'impact est parfaitement insignifiant et marche sur des petites infrastructures tel qu'un blog ou une page web amateur. Pour aller au delà de ces limites, le DDOS doit être parfait. Pour ce faire, il faut de solides compétences en hacking, et des zombies. Mais attendez, des ZOMBIES ???
Oui vous avez bien lu ! Ce que l'on appelle zombie dans le domaine du hacking est en réalité un ordinateur infecté par un cheval de troie qui a pour but de répondre aux requêtes du hackeur.
Pour faire simple, disons que pour lancer une attaque coordonnée, il suffit d'un ou plusieurs hackeurs qui ont sous leurs ordres plusieurs PC distants infectés par leurs programmes. Grâce à cette configuration, chaque hackeur peut envoyer des requêtes aux machines distantes pour « balancer » des paquets vers une cible précise. Vous comprendrez ainsi que plus le parc de systèmes infectés est grand, plus le DDOS est efficace.



il faut de solides compétences en hacking, et des zombies

Comment se protéger des attaques DDOS ?
Ils existe en effet des solutions pour contrer une attaque DDOS, comme nous l'a expliqué notre hébergeur MODEL FX dans un court entretien (Telco = Opérateur Télécom)

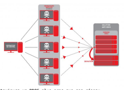
JVL : Avez-vous un moyen de contrer les attaques DDOS, et si oui, jusqu'à quelle « quantité » ?
MFX : Actuellement, nous utilisons une solution basée sur NetFlow qui permet de filtrer jusqu'à 40G.

JVL : Quelles solutions existent pour contrer ces attaques DDOS ?
MFX : Soit une solution basée sur les capacités de mesure et de filtrage des équipements de coeur et de périphérie de réseau (NetFlow, sFlow, etc…) à l'intérieur du réseau de l'hébergeur et qui peuvent représenter une capacité de filtrage proche de la capacité réseau totale (si elle est bien conçue), soit des solutions « cloud » comme CloudFlare (capacité variable en fonction des prestataires, et généralement réservée à des petits volumes), soit des solutions spécialisées comme Arbor PeakFlow. Habituellement les Telco choisissent cette dernière solution car elle permet de filtrer de grosses capacités sur des réseau étendus et de préserver les économies d'échelles qui sont le point fort de ces structures.

JVL : Avez-vous un service « attitré » pour ce problème en particulier ou est-il noyé dans la masse ?
MFX : Pour nos clients en hébergement infogéré, nous avons choisi d'inclure ce service dans la prestation globale.

Si on adopte la solution Arbor (qui nous serait fournie par un Telco, car notre réseau est trop petit pour en tirer vraiment parti, sans parler du coût) il est prévu d'augmenter le prix mensuel de quelques euros, (plus ou moins, en fonction de la valeur de l'offre concernée). Arbor PeakFlow est un système qui permet de traiter de très grandes quantités de flux et de délivrer du traffic « nettoyé » à un client, donc il nous paraît plus logique, à notre échelle, de souscrire ce service auprès d'un Telco qui pourra absorber de gros volumes de traffic « sale » tout en nous livrant des flux « propres » sur un lien de capacité beaucoup plus petite.

L'alternative est de surdimensionner notre réseau, mais il y a toujours un DDOS plus gros que son réseau, comme nous le rappelle régulièrement l'actualité. Personnellement, il me paraît plus économique de déléguer la course aux armements aux Telco et de me concentrer sur le système.



il y a toujours un DDOS plus gros que son réseau

DDOS : Le mot de la fin
Il en ressort au final qu'il n'y a actuellement aucune solution miracle contre les DDOS, les attaques finissent toujours par aboutir même si cela prend des jours. Les solutions apportées par toutes ces entités sont donc parfaites pour des attaques de petite envergure, mais font assez pâle figure devant une attaque coordonnée et de grande ampleur.

Il est difficile d'imaginer que ce ne sera plus qu'un mauvais souvenir dans un avenir proche, car les techniques des hackeurs évoluent avec le temps, et malgré une avancée constante dans le domaine des protections anti-DDOS, rien ne garantit que les pirates n'arriveront finalement pas à leurs fins.

L'histoire nous a, à maintes reprises, prouvée que les hackeurs ont toujours trouvé une solution pour contourner tout type de protection, et même les sociétés d'envergure mondiale nous ont ainsi « démontré » qu'aucun système n'était au final inviolable.

Plus d'infos sur : http://www.jeuxvideo-live.com/dossiers-jeux-video/ddos-un-deebut-de-compreehension/#ixzz3SSMT9mNA

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

Source : http://www.jeuxvideo-live.com/dossiers-jeux-video/ddos-un-deebut-de-compreehension/
Par Spike