Huit bonnes pratiques pour bien sécuriser les objets connectés

Huit bonnes pratiques pour bien sécuriser les objets connectés

Il existe aujourd'hui des failles de sécurité qui permettent d'accéder au capteur, de s'y connecter et d'y collecter des informations. Comment alors se protéger contre de telles intrusions ? Le point.

Gartner prédit 26 milliards d'objets connectés d'ici 2020. En 2016 ce sont 4,9 milliards de dispositifs connectés qui devraient être déployés. Des objets qui seront potentiellement confrontés à un grand nombre d'attaques. En effet, le volume des cyber-attaques recensé par l'étude The Global State of Information Security® Survey 2016, réalisée par le cabinet d'audit et de conseil PwC en collaboration avec CIO et CSO, a progressé de 38 % dans le monde en 2015. Comment alors sécuriser au mieux ses objets connectés ?

En appliquant quelques bonnes pratiques.

Il existe aujourd'hui des failles de sécurité qui permettent d'accéder au capteur, de s'y connecter et d'y collecter des informations. Comment alors se protéger contre de telles intrusions ? Plusieurs zones « sensibles » sont donc à surveiller au sein des objets connectés notamment au niveau du capteur et au niveau du transfert des données.

Pour le capteur, l'un des moyens les plus efficaces pour se protéger consiste à sécuriser le hardware grâce à un Secure Element, qui empêche tout accès à l'information lorsqu'on se connecte au capteur. Un élément sécurisé repose sur une plate-forme matérielle inviolable qui héberge des données, cryptées ou non, en toute sécurité et en conformité avec les règles de sécurité fixées par les autorités de confiance. Certains de ces éléments, comme les cartes microSD, peuvent même être amovibles.

Pour sécuriser les données, il est indispensable d'utiliser des technologies de chiffrement robustes afin de lutter contre le piratage ou les interceptions. En effet, le chiffrement rend les données impossibles à lire pour qui ne possède pas la clé de déchiffrement de 128 bits ! Efficace pour repousser les hackers même les plus coriaces.

Une fois le capteur protégé et les données chiffrées, il est important d'assurer la sécurité de l'information lors de son transfert de bout en bout : du capteur jusqu'au portail client.

L'utilisation d'un système de clés multiples géré par un tiers de confiance tel que le propose le protocole LoRa s'avère une solution des plus fiables.

Un tiers de confiance fournit un système de gestion de clé – Key Management System (KMS) – qui permet de générer une AppKey unique pour chaque capteur. A chaque nouvelle session, une AppSKey – Application Session Key – dérivée de l'AppKey sert au chiffrement des données du client. L'opérateur n'a pas accès à ces 2 clés, elles ne sont connues que du tiers de confiance dans le KMS et du client bien sûr pour déchiffrer les données.

Une fois les données récupérées, l'utilisation d'un VPN est bien sûr conseillé.

En agissant à ces différents niveaux, vous appliquez une sécurité optimale à vos objets connectés. De plus, vous pouvez appliquer quelques conseils pour assurer une sécurité de bout en bout des processus :

1. Évaluez le bon degré de sécurité sur le capteur en fonction de la criticité de la donnée : selon l'information concernée, il n'est pas forcément nécessaire d'insérer un Secure Element dans le capteur.
2. Utilisez une technologie avec un protocole de chiffrement robuste de type AES128 par exemple.
3. Mettez en place des infrastructures intégrant l'état de l'art en termes de chiffrement.
4. N'écrivez pas vos clés de cryptage sur disque dur : privilégiez les éléments de sécurité non stockés et volatiles. Calculées « à la demande » par un algorithme, elles ne peuvent donc pas être piratées en cas d'attaque sur la base de données.
5. Optez pour un renouvellement de la clé de chiffrement à chaque connexion du capteur sur le réseau. Une clé renouvelée régulièrement à moins de risque d'être piratée.
6. Utilisez un portail sécurisé pour accéder à vos données applicatives chiffrées : vous avez ainsi, seul, la possibilité de déchiffrer les données. Toutefois, si vous choisissez de ne pas les déchiffrer vous-même, assurez-vous que votre prestataire le fasse sur un cloud sécurisé.
7. Choisissez des technologies en perpétuelle évolution : au sein de la LoRa Alliance, un groupe dédié fait évoluer en permanence le protocole afin d'être toujours à la pointe de la sécurité.
8. Optez pour un opérateur qui intègre les processus de sécurité recommandés par l'ANSSI dans la conception et l'exploitation de son réseau.

Article original de Franck Moine

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.

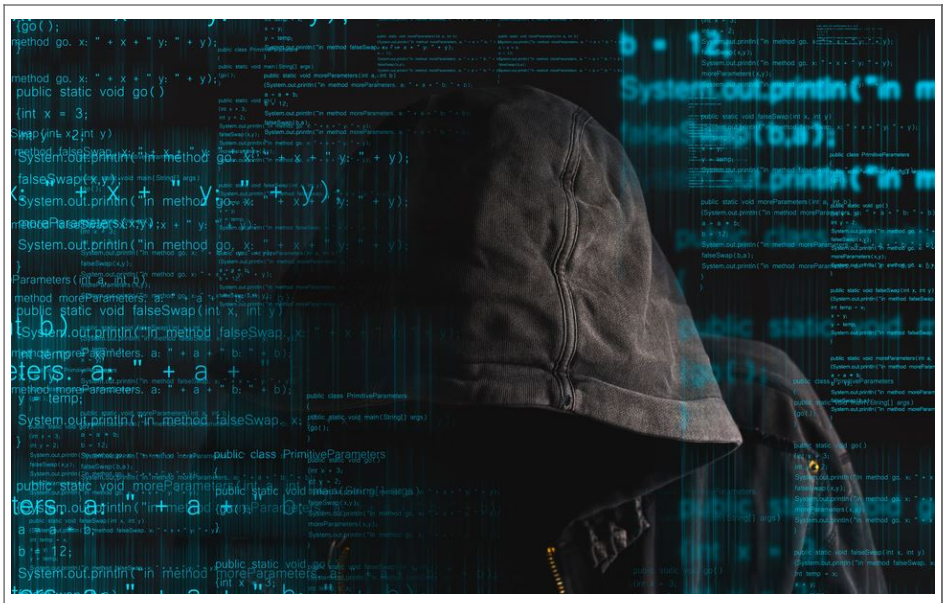
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Huit bonnes pratiques pour bien sécuriser les objets connectés – JDN

Un cousin du malware Furtim cible les énergéticiens européens



Un cousin du malware Furtim cible les énergéticiens européens

---

SentinelOne a découvert une variante du malware Furtim qui vise les sociétés européennes dans le domaine de l'énergie.

En mai dernier, des chercheurs la société EnSilo ont découvert un malware baptisé Furtim qui devait son nom à une obsession virant à la paranoïa de ne pas être détecté par les outils de sécurité. De la préparation à son installation jusqu'à son implémentation, le malware scrute, analyse et bloque tout ce qui touche de près ou de loin à la sécurité IT.

Il semble que ce malware revienne sous une autre forme pour s'attaquer au système industriel des entreprises énergétiques européennes. Des chercheurs de SentinelOne l'ont détecté au sein du réseau d'un énergéticien européen. Cette menace a un nom, SFG, et a été trouvée à la fois par une remontée d'information des logiciels de SentinelOne, mais aussi sur des forums privés. Les experts ont travaillé sur les échantillons pour comprendre son fonctionnement. Les résultats de cette analyse montrent que le comportement, la sophistication et la furtivité du malware sont l'œuvre d'un Etat ou pour le moins d'une organisation soutenue par un gouvernement. Les experts penchent pour une initiative provenant de l'Europe de l'Est.

Jusqu'au sabotage du réseau énergétique

Dans le détail, le cousin de Furtim s'appuie sur les mêmes exploits pour éviter d'être repéré par les outils de sécurité (antivirus, firewall next gen, solution endpoint, sandboxing). Plusieurs développeurs de haut niveau ont mis la main à la pâte pour perfectionner SFG. L'objectif est multiple, extraire des données ou faire tomber le réseau d'énergie, sans laisser de traces. Le malware affecte toutes les versions de Windows, précise SentinelOne dans un blog. Il situe ses débuts au mois de mai dernier et il est encore actif.

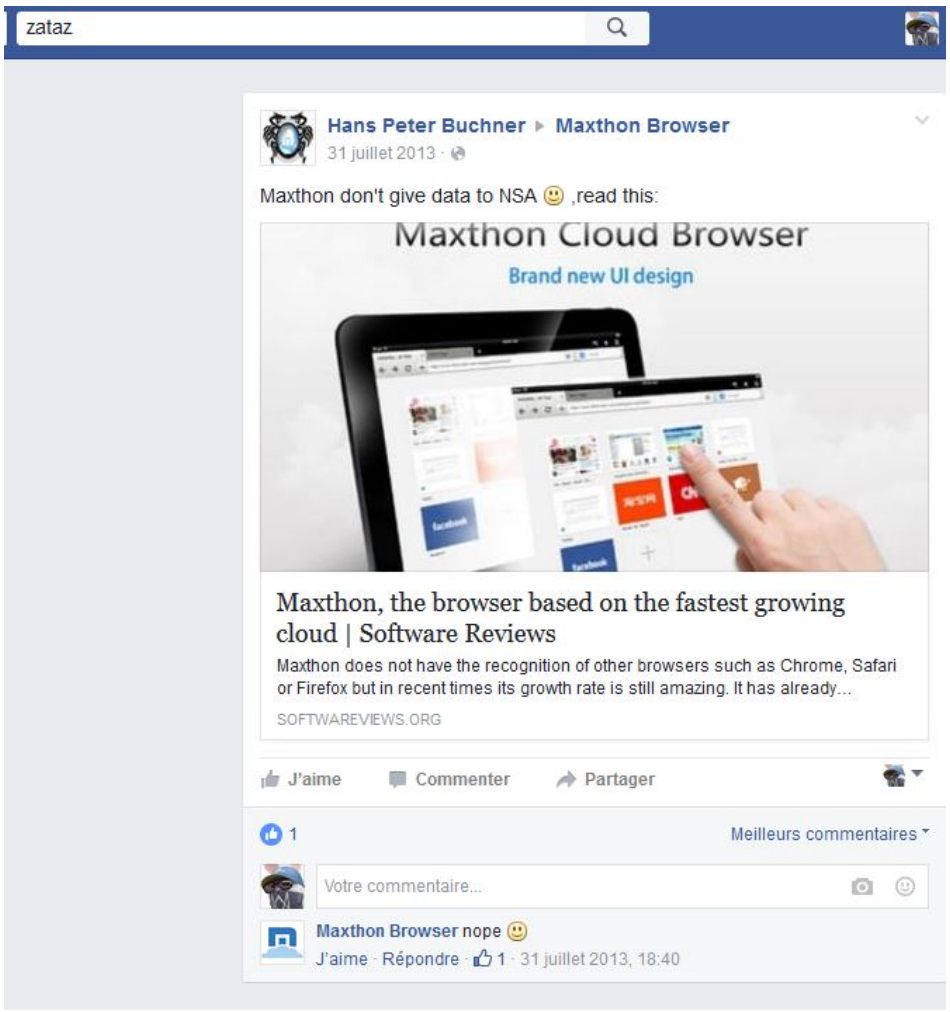
Ce n'est pas la première fois que les entreprises énergétiques sont visées par des malwares ayant pour ambition le sabotage du réseau. On pense bien évidemment au premier virus qui visait les SCADA, Stuxnet. Mais plus récemment, l'Ukraine a été victime d'une panne de courant provoquée par une cyberattaque s'appuyant sur le malware Blackenergy. Ce type de menaces est pris très au sérieux par les gouvernements au point de forcer les entreprises à remonter leurs niveaux de sécurité. En France, l'ANSSI peaufine les arrêtés sectoriels sur la sécurité des OIV (opérateurs d'importance vitale) notamment dans le domaine de l'énergie.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l'article mis en page : Malware : un cousin de Furtim cible les énergéticiens européens

Attention, le navigateur Maxhton espionne ses utilisateurs !



Attention, le navigateur Maxhton espionne ses utilisateurs !

Le navigateur Maxhton ne serait rien d'autre qu'un outil d'espionnage à la solde de la Chine ?

Des experts en sécurité informatiques de l'entreprise polonaise Exatel viennent de révéler la découverte de faits troublant visant le navigateur *Maxhton*. Ce butineur web recueille des informations sensibles appartenant à ses utilisateurs. Des informations qui sont ensuite envoyées à un serveur basé en Chine. Les chercheurs avertissent que les données récoltées pourraient être très précieuses pour des malveillants.

Les données des utilisateurs de Maxhton envoyées en Chine !
Et pour cause ! Les ingénieurs de *Fidelis Cybersecurity* et *Exatel* ont découvert que Maxthon communiquait régulièrement un fichier nommé ueipdata.zip. Le dossier compressé est envoyé en Chine, sur un serveur basé à Beijing, via HTTP. Une analyse plus poussée a révélé que ueipdata.zip contient un fichier crypté nommé dat.txt. Dat.txt stocke des données sur le système d'exploitation, le CPU, le statut ad blocker, l'URL utilisé dans la page d'accueil, les sites web visités par l'utilisateur (y compris les recherches en ligne), et les applications installées et leur numéro de version.
En 2013, après la révélation du cyber espionnage de masse de la NSA, Maxhton se vantait de mettre l'accent sur la vie privée, la sécurité, et l'utilisation d'un cryptage fort pour protéger ses utilisateurs. (Merci à I.Poireau)
Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Le navigateur Maxhton espionne ses utilisateurs – ZATAZ

Un concessionnaire Lamborghini de Mulhouse piraté

Un concessionnaire Lamborghini de Mulhouse piraté

Le vol de données peut souvent cacher des arnaques et attaques informatiques plus vicieuses encore. Exemple avec le piratage d'un concessionnaire de Lamborghini de l'Est de la France.

Derrière un piratage informatique, 99 fois sur 100, se cache le vol des données que le malveillant à pu rencontrer dans son infiltration. Des données qui se retrouvent, dans l'heure, quand ce n'est pas dans les minutes qui suivent la pénétration du site dans des forums et autres boutiques dédiés à l'achat et revente d'informations subtilisées.Un concessionnaire de Lamborghini, à Mulhouse, vient d'en faire les frais.

Une fois les contenus dérobés exploités (phishing, escroqueries…) le pirate s'en débarrasse en les diffusant sur la toile. C'est ce qui vient d'arriver à un concessionnaire automobile de l'Est de la France. Ici, nous ne parlons pas de la voiture de monsieur et madame tout le monde, mais de Lamborghini.

Prend son site web par dessus la jambe et finir piraté !

Le concessionnaire se retrouve avec l'ensemble des pousses bouton de la planète aux fesses. De petits pirates en mal de reconnaissance qui profitent d'une idiote injection SQL aussi grosse que l'ego surdimensionné de ces « piratins ». Bilan, le premier pirate a vidé le site, revendu/exploité les données. Il a ensuite tout balancé sur la toile. Les « suiveurs » se sont jetés sur la faille et les données. J'ai pu constater des identifiants de connexion (logins, mots de passe) ou encore des adresses électroniques lâchées en pâture. Des courriels internes (webmaster, responsables du site…).

Article original de Damien Bancal

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 : ZATAZ Un concessionnaire Lamborghini de Mulhouse piraté – ZATAZ

Google met en avant ses succès contre le piratage

Google met en avant ses succès contre le piratage

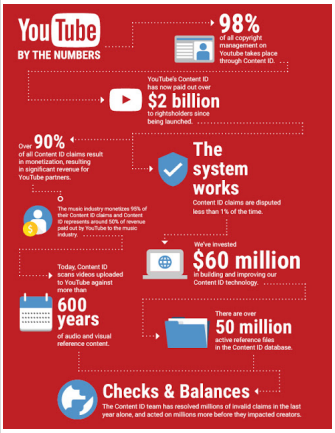
Google combat le piratage, et cherche de plus en plus à le faire savoir. En plus de son filtrage qui limite l'utilisation de Google pour trouver des contenus piratés, Google a reversé 2 milliards de dollars aux ayants droits dont les contenus ont été mis en ligne sur YouTube. Difficile, toutefois, de savoir si c'est beaucoup… ou très peu.
Depuis plusieurs années, Google aime à s'afficher comme défenseur des droits d'auteur, alors que le moteur de recherche a souvent été vilipendé par des ayants droit qui lui reprochaient de donner trop facilement accès à des sites pirates. La firme de Mountain View, qui doit soigner des partenaires commerciaux pour YouTube et pour ses services de distributions de contenus sur Google Play, publie même désormais un document de 62 pages pour expliquer « Comment Google combat le piratage ».

Sur son blog dédié aux politiques publiques, Google précise certains points qui ont été mis à jour dans ce document, lequel était inimaginable quand les recherches avec des mots clés comme « torrents », « mp4 » ou « streaming » renvoyaient encore le plus souvent vers des pages de sites pirates.
NOS ALGORITHMES DE CLASSEMENT DES RECHERCHES RÉTROGRADENT CE SITE DANS LES FUTURS RÉSULTATS DE RECHERCHE

Aujourd'hui, « la grande majorité des requêtes liées à des médias que les utilisateurs soumettent chaque jour retournent des résultats qui incluent seulement des liens vers des sites légitimes », se félicite le géant de la recherche. Et lorsque l'utilisateur cherche à forcer la recherche avant des mots clés spécifiques au streaming gratuit ou au téléchargement sur BitTorrent, « nos systèmes de traitement des demandes de suppressions pour violation du droit d'auteur gèrent des millions d'URL chaque jour », qui font qu'en cas d'infractions répétées sur un site, « nos algorithmes de classement des recherches rétrogradent ce site dans les futurs résultats de recherche ».

2 MILLIARDS DE DOLLARS REVERSÉS PAR YOUTUBE AUX AYANTS DROITS

*Sur YouTube, la chasse au piratage et aux utilisations non autorisées d'extraits de vidéos ou de musique est fortement automatisée, avec **Content ID** qui détecte les empreintes des contenus et permet aux ayants droit de choisir, soit la suppression des exploitations illégales, soit de recevoir les revenus publicitaires attachés à cette exploitation – ce qui n'est pas sans poser régulièrement quelques problèmes de retraits abusifs ou de détournement de revenus par des ayants droits qui s'accaparent toute œuvre dérivée.*
*Ainsi selon Google, 98 % des problèmes de droits d'auteur sur YouTube sont désormais gérés directement avec Content ID, ce qui ne laisse que 2 % de demandes de suppression envoyées par formulaire. **Dans 90 % des cas les ayants droit choisissent de percevoir une rémunération** plutôt que demander le retrait des vidéos mises en cause.*
*Google dit ainsi avoir versé 2 milliards de dollars de droits grâce à Content ID depuis son lancement, ce qui est beaucoup et peu à la fois. Il ne dit pas à combien de visionnages cela correspond, ce qui ne permet pas de calculer le gain par vidéo vue. La **page officielle des statistiques de YouTube**, dont la mise à jour ne semble pas récente, indique que « depuis juillet 2015, plus de 8 000 partenaires (parmi lesquels de nombreux grands groupes audiovisuels, studios de cinéma et maisons de disques) ont revendiqué plus de 400 millions de vidéos via Content ID ».*
Le système est aujourd'hui capable de détecter 50 millions d'œuvres, réattribuées à leurs propriétaires respectifs en cas de réclamation.



Article original de Guillaume Champeau

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 : Google met en avant ses succès contre le piratage – Politique – Numerama

---

Attention aux versions piégées de Pokémon GO

Attention aux versions piégées de Pokémon GO

L'application Pokémon Go fait un carton dans les smartphones. Prudence, non encore officiel en Europe, installer le jeu via des boutiques hors de contrôle des auteurs met en danger votre vie privée.

Pas de doute, le phénomène Pokémon GO débarque en force en cet été 2016. L'application tirée du jeu éponyme de Nintendo permet de s'éclater à trouver des Pokemons un peu partout dans le monde. De la réalité virtuelle bien venue pour l'été.

Édité par Niantic, le créateur de Pokémon GO ne propose son appli qu'aux États-Unis, en Australie et en Nouvelle-Zélande. Un pré lancement pour tester les serveurs, très sollicités, et la stabilité du jeu. Bref, normalement, il n'est pas possible d'y jouer en Europe, et donc en France. Sauf qu'il y a toujours des possibilités, comme celle d'installer Pokémon GO vient l'APK (le programme) proposé par de nombreux sites Internet non officiels.

Attention ! des sites qui ne sont pas maîtrisés et contrôlés par les auteurs. Des espaces de téléchargements qui sont des limites du Play Store de Google et de l'App Store d'Apple. Bref, à vos risques et périls.

J'ai déjà pu repérer des APK piégés (ransomwares, cheval de Troie, …) proposés, je l'avoue, dans des lieux peu recommandables. Prenez l'avertissement très au sérieux. Pokemon GO ne vous demandera JAMAIS d'accéder à vos messages [SMS, MMS], à vos appels téléphoniques. Si l'APK que vous avez téléchargez vous propose ces « autorisations », ne l'installez surtout pas. Attendez la version officielle.

Je ne me voile pas la face, le phénomène attire beaucoup d'internautes, jeunes et moins jeunes. Et avec les vacances, une bonne occasion de sauter sur le jeu pour smartphone de l'été. Des milliers de Français l'ont fait. J'en croise beaucoup, dans la rue, comme le montre ma photographie, prise ce 13 juillet dans les rues de Paris. Je rentre de New York, l'engouement est… pire !

A noter que plusieurs éditeurs d'antivirus ont mis la main sur une version « malveillante » de Pokémon GO. Bitdefender, par exemple, parle de DroidJack. Ce cheval de Troie ouvre une backdoor et donne l'accès aux données des appareils mobiles infectés, permettant ainsi leur prise de contrôle à distance par les pirates. Ce malware disponible pour seulement 200 dollars sur certains sites Web, offre au pirate une interface de contrôle facile à utiliser lui permettant par exemple de surveiller l'activité des appareils corrompus, de passer des appels, d'envoyer des SMS, de localiser l'appareil, d'utiliser l'appareil photo ou le microphone ou même d'accéder aux dossiers.

La version iPhone malmenée par la version officielle

Autre mise en garde pour les joueurs de Pokémon GO : sur iOS, l'application semble demander plus d'autorisations que nécessaire. L'accès à l'application via un compte Google semble conférer au développeur Niantic (ex Start-up de Google), un accès complet aux comptes des utilisateurs. Ce problème est en cours de résolution et n'est pas présent dans les versions Android.

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Pokémon GO, prudence aux fichiers vérolés – ZATAZ

L’accord sur la transmission des données validé par la Commission Européenne

	L’accord sur la transmission des données validé par la Commission Européenne – Filière 3e

---

Le 8 juillet, la Commission européenne a validé le projet des représentants des Etats-membres de l'UE et des Etats Unis sur le transfert des données en ligne. Une législation qui pourrait favoriser l'Open Data, les objets connectés ainsi que la mise en place de projets de transition énergétique.

A l'origine l'accord sur la transmission des données était appelé « Safe Harbour ». La Cour de Justice de l'Union européenne (CJUE) avait invalidé le texte en octobre 2015 en raison de sa faible sécurité pour les données personnelles. Après des mois de débats, l'accord sur la « protection de la vie privée » (Privacy Shield) a été approuvé par les Etats membres et est entré en vigueur le 11 juillet 2016. Il a pour but de faciliter le transfert des données entre les Etats-Unis et l'Union européenne dans le cadre de la signature du Traité Transatlantique (TAFTA ou TIPP). Ce texte a pour but de faciliter les échanges économiques entre l'UE et les Etats-Unis, en harmonisant les normes européennes à celles américaines. Ces échanges serviraient à encadrer le progrès dans la croissance économique, en favorisant les flux correspondant au secteur du numérique. Dans un communiqué de presse, Andrus Ansip, membre désigné de la Commission Juncker comme vice-président chargé du marché numérique, et la commissaire à la Justice, Vera Jourva, ont déclaré communément : « le texte est fondamentalement différent de l'ancien Safe Harbour: il impose des obligations claires et fortes aux entreprises traitant les données et s'assure que ces règles sont suivies et mises en pratique ».

L'Open Data utile à la transition énergétique ?

Largement décriée, la récupération des données servira pourtant à construire le monde de demain en s'inscrivant dans une logique de transition énergétique. Ainsi les villes, les maisons et les énergies fonctionneront dans un même système connecté et durable. Nombreuses sont les start-up a créer des applications facilitant la mobilité, la sécurité et l'habitat dans le cadre de projets « verts ». Les données deviennent un facteur important du marché économique et énergétique. Pour Christian Buchel, Directeur général adjoint, Chef digital et international pour le groupe ENEDIS : « l'Open Data est utilisé dans le monde entier. Humaniser la DATA c'est mieux comprendre la consommation générale d'énergie ». Des informations qui pourraient être utilisées à grande échelle afin d'accroître la capacité de gestion des énergies. L'anonymat des données serait préservé puisque seul le consommateur aurait accès à ses informations. Pour Sampo Hietanen, de MAAS Finlande, une entreprise spécialisée dans l'Open DATA, il faut « générer de l'information pour construire la ville de demain afin que les services proposés communiquent ensemble ».
Les Etats Unis ont déjà commencé à déployer ce système numérique avec la mise en place de compteurs intelligents, récupérant les données des citoyens pour adapter la consommation énergétique à la demande. La France et ERDF commencent à commercialiser Linky, le compteur intelligent français. En ce sens, la signature du Traité Transatlantique devrait favorisait les partenariats énergétiques et numériques entre l'Union Européenne et les Etats-Unis.
Article original de Mailys Kerhoas

Réagissez à cet article

Original de l'article mis en page : L'accord sur la transmission des données validé par la Commission Européenne — Filière 3e

---

Le Maroc peut-il créer une

Silicon Valley au Maghreb ?

Le Maroc peut-il créer une Silicon Valley au Maghreb ?

Le Maroc a-t-il les capacités de se transformer en « Silicon Valley » du Maghreb? Hamza Hraoui, conseiller en communication d'influence pour les entreprises et les dirigeants, estime que »oui ».

Dans un entretien paru jeudi 7 juillet au HuffpostMaroc, cet expert estime que le Maroc a toutes les potentialités pour cet objectif, à condition de revoir le fonctionnement de l'Agence nationale de réglementation des télécommunications (ANRT). »Nous sommes en tout cas crédibles et légitimes pour être le spot technologique de la région », souligne t-il. »Le taux de pénétration d'internet dépasse 56% chez nous alors qu'en Tunisie c'est 44%, en Algérie c'est moins de 20%. En plus d'avoir la population la plus connectée du Maghreb, le Maroc connaît également le plus fort dynamisme de ses médias en ligne. » En outre, le Maroc a pris de l'avance sur le plan des infrastructures de TIC, selon lui: » quand l'Algérie a introduit la 3G qu'en 2013, nous avons aujourd'hui la couverture 4G la plus large du Maghreb. » Mais, tempère l'expert, le pays accuse déjà un retard dans ce domaine.

Le »Hic »

»Au Maroc on est au point mort », affirme t-il, avant d'expliquer que »si la stratégie industrielle (du Ministre de l'Industrie et de l'Economie numérique) a esquissé les grandes lignes de l'économie numérique du pays, la structuration des écosystèmes numériques tarde à venir », même si »le potentiel est là. » Pour Hamza Hraoui, »il faut enclencher maintenant notre transformation et prendre le train de la nouvelle économie en misant sur notre tissu entrepreneurial. » Car »les Marocains attendent un vrai plan du numérique, conquérant et volontariste qui permettra d'accompagner les projets structurants des entreprises sur les marchés, où le Maroc peut acquérir d'ici 3 à 5 ans, un leadership continental: fabrication additive comme les imprimantes 3D, les objets connectés, la réalité augmentée, les villes intelligentes, les écoles du numérique… » Pour cela, il faut que bien des barrières tombent, et que les opérateurs du secteur rattrapent le retard accusé par le Maroc dans le digital et l'économie numérique.

Faire sauter les barrières

Et, surtout, libérer le secteur des »interdits » et des blocages. Il estime ainsi que la Maroc, en interdiction de la VoiP, »donne un mauvais signal aux acteurs de la nouvelle économie suite à cette interdiction. » »Et ses répercussions se feront sentir à moyen et à long terme », ajoute cet expert en communication, qui appelle l'ANRT à faire »son update ». Plus direct, il accuse l'ANRT de cloisonner le secteur des TIC et empêcher l'économie numérique de se développer. »A l'heure du décloisonnement de l'information, de l'explosion de la data et de l'émergence de l'économie collaborative, l'ANRT poussée et pressée par les opérateurs télécom, nous a montré qu'elle vit encore à l'âge de pierre en enlevant aux jeunes étudiants, aux chercheurs, aux start-upers qui créent de la richesse dans ce pays l'essence même du progrès: le droit à la mobilité. » Pour lui, »cela nous montre à quel point nos institutions ont du mal à admettre que la relation public-autorité et l'ordre établi sont profondément bouleversés par le digital, obligeant les hommes politiques à revoir en profondeur leurs messages, décisions et façons de faire. » A fin décembre 2015, le Maroc comptait 13,89 millions d'abonnés à l'Internet fixe, soit un taux de pénétration de 41,1 %, alors que le parc de l'internet mobile compte 12,81 millions d'abonnés avec une progression de 69,58% par an.

Article original de Amin Fassi-Fihri

Réagissez à cet article

Original de l'article mis en page : TIC: Le Maroc peut créer une Silicon Valley au Maghreb, mais…(Expert) – Maghreb Emergent

Secret des conversations, Facebook Messenger bientôt chiffré

	Secret des conversations, Facebook Messenger bientôt chiffré

Non, tous les échanges sur Messenger ne sont pas chiffrés de bout en bout. Pas encore du moins. Facebook teste le procédé à travers une nouvelle fonctionnalité, #Secret Conversations. En y ajoutant un petit côté messages éphémères à la Snapchat.

Facebook chantre du chiffrement de bout en bout ? L'entreprise vient de lancer une nouvelle option pour Messenger permettant de démarrer une conversation sécurisée. Baptisée Secret Conversations, celle-ci permet de créer, via la fiche d'un contact, une conversation chiffrée entre deux utilisateurs. Derrière, on retrouve le protocole Signal, également utilisé par WhatsApp.
Mais, contrairement à #WhatsApp, Secret Conversations se veut optionnel, pour ne pas dire ponctuel. Car il s'agit là de préférer la sécurité au confort, un choix auquel Facebook n'entend pas contraindre ses utilisateurs. Ainsi, via cette fonctionnalité, on ne peut envoyer que du texte et des photos à un unique destinataire. Pas de vidéo, de GIF, de paiement ou de discussion de groupe.

Ce message s'autodétruira automatiquement dans 4…3…

Cette sobriété se conjugue avec l'absence de synchronisation entre les appareils d'un même utilisateur. Impossible donc de commencer une conversation chiffrée avec son iPhone et de passer ensuite à sa tablette : la discussion est uniquement rattachée au terminal avec lequel elle a été initiée. En outre, preuve que Mark Zuckerberg n'a toujours pas digéré le refus de son offre de rachat sur Snapchat, il est possible de définir à l'aide d'un minuteur la durée de vie d'un message. Qui s'autodétruira une fois le délai écoulé.
L'option est intégrée à l'application Messenger pour Android et iOS. Déjà disponible pour certains, elle sera déployée plus largement au cours de l'été. Pour l'heure, il semble que rien ne soit prévu pour les versions navigateur du service.

Article original de Guillaume Périssat

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 : Secret Conversations : Facebook Messenger en mode chiffré

Le malware Nymaim s’attaque désormais aux institutions financières du Brésil

Le malware Nymaim s’attaque désormais aux institutions financières du Brésil

Après avoir contaminé l'Europe et l'Amérique du Nord en 2013, le malware Nymaim refait surface 3 ans plus tard et se propage désormais via une campagne de spearphising intensive, en utilisant un document Microsoft Word comme pièce jointe infectée

Lors de la découverte de la souche originale de Nymaim en 2013, notamment avec ses techniques de code modulaire (chaîne d'abattage et d'évasion), nous avions pu remarquer que plus de 2,8 millions d'infections s'étaient propagées. Sur le premier semestre 2016, ESET a de nouveau observé une augmentation significative de détections du malware Nymaim.

Infectant principalement la Pologne (54%), l'Allemagne (16%) et les Etats-Unis (12%), cette mutation du malware Nymaim a été détectée comme appartenant à la catégorie *Win32/TrojanDownloader.Nymaim.BA.* Elle utilise le spearphishing et une pièce jointe (type Word.doc) contenant une macro malveillante. Utilisée pour contourner les paramètres de sécurité par défaut de Microsoft Word via les techniques d'ingénierie sociale, l'approche est très dangereuse dans les versions anglaises de MS Word.

« Grâce à ses techniques d'évasion sophistiquées, l'anti-VM, l'anti-débogage et les flux de contrôle, cette fusée à deux étages sert à livrer le ransomware comme charge utile finale. Ce code que l'on peut nommer « Trojan modulaire » est impressionnant par sa faculté à voler les informations d'authentification de sites de banque électroniques dans les formulaires typiques en contournant la protection SSL. Ce code malveillant a évolué de façon à fournir des logiciels espions », explique Cassius de Oliveira Puodzius, Security Researcher chez ESET en Amérique Latine.

En avril 2016, la version précitée a été rejointe par une variante hybride de Nymaim (Gozi) qui avait pour cible les institutions financières d'Amérique du Nord, mais également en Amérique latine et principalement au Brésil. Cette variante fournit aux cybercriminels le contrôle à distance des ordinateurs compromis plutôt que de chiffrer les fichiers ou bloquer la machine – comme cela se fait habituellement.

En raison des similitudes entre les cibles visées dans chaque pays et les taux de détection, nous pouvons affirmer que les institutions financières restent au centre de cette campagne.

« L'étude complète de cette menace est toujours en cours. Toutefois, si vous pensez que votre ordinateur ou votre réseau a été compromis, nous vous recommandons de vérifier que les adresses IP et les URL que nous avons partagées dans l'article complet de WeLiveSecurity ne se trouvent pas dans votre pare-feu et dans le journal de votre proxy. Nous vous conseillons de mettre en place une stratégie de prévention en ajoutant une liste noire des des adresses IP contactées par ce malware au pare-feu et les URL à un proxy, aussi longtemps que votre réseau prendra en charge ce type de filtrage », conclut Cassius de Oliveira Puodzius.

Pour lire l'intégralité du rapport et ainsi obtenir des informations complémentaires sur le malware Nymaim, cliquez ici.

Réagissez à cet article