Connaissez-vous le réseau plus anonyme et rapide que Tor ?

	Connaissez-vous le réseau plus anonyme et rapide que Tor ?

Le Massachusetts Institute of technology (MIT), aux États-Unis, et l'École polytechnique fédérale de Lausanne (EPFL), en Suisse, annoncent la création d'un nouveau réseau anonyme sur Internet, baptisé Riffle, encore plus rapide et sécurisé que Tor, la référence en la matière.

A l'image de Tor, le plus célèbre des réseaux de ce type, Riffle permet de surfer et de communiquer en théorie en parfait anonymat en s'appuyant sur le protocole de chiffrement "en oignon". Cela signifie qu'il est composé d'une multitude de couches de routeurs, autant de "noeuds" par lesquels transitent les flux d'informations sur le réseau, garantissant ainsi l'anonymat de ses utilisateurs. Les données personnelles de l'internaute (adresse IP, pays) ne peuvent ainsi plus être localisées par les sites visités. Cette alternative serait toutefois selon ses créateurs bien plus sécurisée et fiable que Tor et consorts.
Selon le MIT, l'avantage de Riffle repose sur ses serveurs, capables de permuter l'ordre de réception des messages rendant l'analyse du trafic encore plus complexe et favorisant donc l'anonymat des utilisateurs. Si, par exemple, les messages provenant d'expéditeurs Alice, Bob et Carol atteignent le premier serveur dans l'ordre A, B, C, ils peuvent être renvoyés dans un ordre complètement différent au serveur suivant, et ainsi de suite. Les utilisateurs du réseau deviennent alors en théorie parfaitement impossibles à identifier.
Dernier point non négligeable, Riffle proposerait une meilleure bande passante, garantissant une navigation plus fluide et des échanges de fichiers accélérés.
Cette annonce intervient alors que la sécurité de Tor a récemment été mise à mal par des chercheurs de la Northeastern University de Boston (États-Unis) qui a découvert plus d'une centaine de "nœuds-espions", en réalité des serveurs, capables d'identifier des services cachés et éventuellement de les pirater.
Davantage de détails sur Riffle, toujours en phase de développement, seront communiqués lors de sa présentation officielle à la conférence Privacy Enhancing Technologies Symposium (PETS), qui se déroulera du 19 au 22 Juillet à Darmstadt (Allemagne).
Article original de Etienne Froment

Réagissez à cet article

Original de l'article mis en page : Riffle, le nouveau réseau garanti plus anonyme et rapide que Tor | geeko

Privacy Shield : 1 an de sursis donné par les CNIL européennes

Privacy Shield : 1 an de sursis donné par les CNIL européennes

Les CNIL européennes ne sont pas satisfaites du Privacy Shield, mais prennent date en 2017 pour s'inviter dans la révision de l'accord.

Le verdict était attendu. Les CNIL européennes du groupe de l'article 29 (G29) ont rendu leur décision définitive sur le Privacy Shield. Cet accord encadre le transfert des données entre les Etats-Unis et l'Union européenne Il est le successeur du Safe Harbor, invalidé par la Cour de Justice de l'Union européenne. Dans un communiqué de presse, le G29 souligne ses réserves sur le Privacy Shield. Il considère néanmoins que l'accord a été voté et il donne rendez-vous au 1 an de l'accord lors de sa révision pour un examen plus approfondi de certaines dispositions.

En avril dernier, le groupe avait émis différentes critiques sur le Privacy Shield. Il avait souligné *« un manque de clarté général »*, une *« complexité »*, et parfois une *« incohérence »*, des documents et annexes qui composent le Privacy Shield. C'est notamment le cas pour les voies de recours que pourront emprunter les citoyens européens contestant l'exploitation de leurs données outre-Atlantique, indique le groupe dans son avis consultatif.

Quant à l'accès des agences de renseignement aux données transférées dans le cadre du Privacy Shield (volet sécurité nationale), il soulève de *« fortes préoccupations »*. Le risque d'une collecte *« massive et indiscriminée »* des données par un État n'est pas écarté. Le groupe s'inquiète aussi du statut et de l'indépendance du médiateur (*« ombudsman »*) vers lequel les citoyens européens pourront se tourner.

Un an de sursis et une mise en garde

Certaines réserves ont été prises en compte, note le G29, mais « cependant un certain nombre de préoccupations demeurent ». Au premier rang desquels, le risque toujours bien réel d'une surveillance de masse par le gouvernement américain. Il évoque le rôle du médiateur et la révision annuelle de l'accord.

Les CNIL européennes comptent beaucoup sur cette révision annuelle prévue en juillet 2017. Elles profiteront de cette occasion « *pour non seulement évaluer si les questions en suspens ont été résolues, mais aussi si les garanties prévues par le Privacy Shield entre les Etats-Unis et l'UE sont réalisées et efficaces* ». Et de prévenir, que « *tous les membres de l'équipe en charge de cette révision doivent avoir accès à toutes les informations nécessaires à l'accomplissement de leur examen y compris des éléments favorisant leur propre évaluation sur la proportionnalité et la nécessité de la collecte et l'accès aux données par les pouvoirs publics* ». Une mise en garde contre les risques d'être éconduits dans un an.

Pendant ce temps-là, le Privacy Shield pourrait être contesté par des citoyens européens, comme cela a été le cas avec Max Schrems pour le Safe Harbor. Lors d'une récente discussion dans le cadre de Cloud Confidence, le jeune avocat avais émis l'hypothèse d'une nouvelle action en justice contre le Privacy Shield.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : Privacy Shield : les CNIL européennes accordent 1 an de sursis

---

Jeux Olympiques de Rio : OP Hashtag infiltre des terroristes

Jeux Olympiques de Rio : OP Hashtag infiltre des terroristes

Op hashtag – La police fédérale Brésilienne aurait infiltré le WhatsApp et Telegram utilisaient par des terroristes locaux. Plusieurs groupes échangeaient des informations sur des tactiques de guerre. Des attentats prévus lors des Jeux Olympiques de Rio ?

Un nouveau cheval de bataille pour la justice brésilienne qui tente de contrôler les réseaux sociaux au Brésil. J'apprends dans le journal brésilien blasting news que La police fédérale brésilienne aurait infiltré le WhatsApp et Telegram de terroristes locaux lors d'une opération baptisée Op Hashtag. Plusieurs personnes s'échangeaient des informations sur des tactiques de guerre. Dans ce nouveau cas, la police fédérale parle clairement de « djihadiste » qui fomentaient des attaques à l'occasion des Jeux Olympique de Rio.

Opération HashTag

L'opération « Hashtag » a été lancée dans la matinée du jeudi 21 juillet. Cette action policière démontre comment la police fédérale aurait réussi à avoir accès aux messages de plusieurs groupes de « terroristes ». Des commanditaires d'attaques en Europe, qui souhaiteraient agir au Brésil.
Alexandre Moraes, le ministre de la Justice, a expliqué que la police tentait de surveiller les conversations WhatsApp. Action difficile puisque tous les messages sont chiffrés « ce qui rend impossible pour quiconque d'avoir accès, y compris à la justice« . Cependant, l'infiltration avec la création de faux comptes d'internautes aurait porté ses fruits. Le ministre a refusé de donner des détails sur la façon dont l'enquête a été menée, mais comme il est impossible de surveiller les messages échangés dans l'application, il est certain que les agents de police se sont présentés comme des candidats brésiliens aux actes assassins réclamaient par Daesh, Al Qaeda …
La Cour fédérale du Paraná a lancé 12 mandats d'arrêt grâce aux enregistrements téléphoniques d'internautes qui se seraient déclarés prêts à orchestrer des attaques lors des JO de Rio. Des internautes qui s'échangeaient aussi des modes d'emploi de tactiques militaires. Le ministre de la Justice a également révélé que certains des brésiliens arrêtés lors de l'Opération Hashtag avaient prêtés serment d'allégeance à l'État islamique.

Contrôler les réseaux sociaux

Le Brésil est précurseur sur de nombreux points concernant le contrôle des réseaux sociaux. Ce pays, qui est un immense vivier de pirates informatiques, tente aussi de cyber surveiller les propos et les internautes passant par ses Internet. Souvenez-vous, en juin 2014, lors de la coupe du monde football, les cyber manifestations lancées par Anonymous. Plus proche de nous, décembre 2015, avec le blocage de WhatsApp durant 48 heures. Un troisième blocage interviendra en mai 2016. Sans oublier l'arrestation d'un dirigeant de Facebook.
Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Jeux Olympiques de Rio : OP Hashtag infiltre des terroristes – ZATAZ

Tor envahi par des mouchards

?

Tor envahi par des mouchards ?

Selon des chercheurs, 110 relais du réseau d'anonymisation Tor étaient à la recherche d'informations sur les services cachés auxquels ils permettent d'accéder.

Deux chercheurs de la Northeastern University (Boston), Guevara Noubir et Amirali Sanatinia, démontrent à leur tour que le réseau Tor est la cible d'espions. Cette fois, les chercheurs n'ont pas étudié des noeuds de sortie détournés pour mener des attaques de type « *Man In The Middle* ». Ils se sont intéressés à d'autres relais : ceux qui permettent d'accéder à des services cachés et référencent des éléments clés (adresse en .onion, clé publique, points d'introduction) .

Ces relais (HSDirs, *Hidden Service Directories*) font partie intégrante des services cachés et du dark web. Mais des entités (gouvernements, entreprises, hackers, etc.) peuvent en modifier le code pour obtenir des informations, découvrir une adresse ou exploiter une faille.

Pot de miel

Dans le cadre de leurs travaux, les chercheurs ont déployé 4500 services cachés (en .onion), 72 jours durant. « *Nos résultats expérimentaux montrent que, durant cette période, au moins 110 relais (HSDirs) étaient à la recherche d'informations sur les services cachés qu'ils accueillent* », soulignent les chercheurs dans une note. Ils ont également indiqué à *Motherboard* que la recherche de vulnérabilités n'est pas exclue des motivations de ceux qui pilotent ces relais. La plupart d'entre eux sont hébergés aux États-Unis, en Allemagne et en France. Mais il est toujours possible d'opérer un serveur à distance…

Roger Dingledine, cofondateur du projet Tor, a expliqué au magazine que peu, voire aucun de ces relais ne se trouvent dans le réseau Tor en ce moment. Le projet travaille, par ailleurs, à la mise en place d'une prochaine génération de services « *onion* ». Quant aux chercheurs, ils présenteront leurs travaux lors de la Defcon 24, qui se déroulera du 4 au 7 août prochains à Las Vegas.

Article original de Ariane Beky

Original de l'article mis en page : Tor envahi par des noeuds espions ?

Détecter les futurs terroristes sur Internet ? L'Europe veut s'inspirer d'Israël

Détecter les futurs terroristes sur Internet ? L'Europe veut s'inspirer d'Israël

Le coordinateur de l'anti-terrorisme pour lUnion européenne, Gilles de Kerchove, s'est rendu en Israël pour trouver des solutions technologiques qui permettraient de détecter automatiquement des profils suspects sur les réseaux sociaux, grâce à des algorithmes de plus en plus intrusifs.

Plus les attentats en Europe se multiplient, plus on découvre que les profils psychologiques et sociaux des kamikazes et de leurs associés sont très divers, jusqu'à paraître indétectables. Le cas de Mohamed Lahouaiej-Bouhlel, dont on ne sait pas toujours très bien s'il s'agit d'un déséquilibré qui se cherchait un modèle ultra-violent à imiter, ou d'un véritable djihadiste islamiste radicalisé à une vitesse inédite, laisse songeur. Bisexuel, amant d'un homme de 73 ans, mangeur de porc, aucune connexion connue avec des réseaux islamistes… l'auteur de l'attentat de Nice était connu des services de police pour des faits de violence de droit commun, mais n'avait rien de l'homme que l'on pourrait soupçonner d'organiser une tuerie motivée par des considérations idéologiques.
Or c'est un problème pour les services de renseignement à qui l'on demande désormais l'impossible, à la Minority Report, c'est-à-dire de connaître à l'avance le passage à l'acte d'un individu, pour être capable de l'appréhender avant son méfait, même lorsqu'objectivement rien ne permettait de présager l'horreur.

C'EST POUR ÇA QUE JE SUIS ICI. NOUS SAVONS QU'ISRAËL A DÉVELOPPÉ BEAUCOUP DE MOYENS DANS LE CYBER

Néanmoins, l'Union européenne ne veut pas se résoudre à la fatalité, et va chercher en Israël les méthodes à appliquer pour détecter sur Internet les terroristes susceptibles un jour de passer à l'acte. « C'est un défi », explique ainsi à l'agence Reuters Gilles de Kerchove, le coordinateur de l'UE pour l'anti-terrorisme, en marge d'une conférence sur le renseignement à Tel Aviv. « Nous allons trouver bientôt des moyens d'être beaucoup plus automatisé » dans la détection des profils suspects sur les réseaux sociaux, explique-t-il. « C'est pour ça que je suis ici ».
« Nous savons qu'Israël a développé beaucoup de moyens dans le cyber », pour faire face aux attaques d'Israéliens par des Palestiniens, ajoute le haut fonctionnaire européen, et l'UE veut s'en inspirer.

ÉTABLIR DES PROFILS SOCIOLOGIQUES ET SURVEILLER LES COMMUNICATIONS

Selon un officiel israélien interrogé par l'agence de presse, il s'agit d'établir constamment des profils types de personnes à suspecter, en s'intéressant non plus seulement aux métadonnées qui renseignent sur le contexte des communications et les habitudes d'un individu, mais bien sur le contenu-même des communications sur les réseaux sociaux.
Mis à jour quotidiennement au gré des nouveaux profils qui émergent, des paramètres comme l'âge de l'internaute, sa religion, son origine socio-économique et ses liens avec d'autres suspects, seraient aussi pris en compte par les algorithmes israéliens – ce qui semble difficilement compatible en Europe avec les textes internationaux protégeant les droits de l'homme, que l'Union européenne s'est engagée à respecter.

DES BOÎTES NOIRES TOUJOURS PLUS INTRUSIVES ?

En somme, c'est exactement ce que nous redoutions avec les fameuses boîtes noires permises par la loi Renseignement en France, dont le Conseil constitutionnel n'a su que dire, et qui se limitent officiellement aux métadonnées. Là aussi, il s'agit d'utiliser des algorithmes, dont on ne sait pas du tout sur quoi ils se basent, pour détecter des profils suspects.

Eagle Security & Defense, une société israélienne proposant des solutions de surveillance sur Internet, a reçu la visite de Christian Estrosi en début d'année.
Il n'est toutefois pas dit que la technologie israélienne soit importée telle quelle, d'autant que M. De Kerchove a lui-même rappelé que le droit européen n'autoriserait pas un tel degré d'intrusion dans la vie privée. Mais le mécanisme décrit par l'officiel d'Israël est très proche.
Il vise tout d'abord à réaliser une première détection sommaire des profils suspects, puis à déterminer parmi eux ceux qui doivent faire l'objet d'une surveillance individualisée. C'est exactement ce que prévoit la loi Renseignement, qui autorise l'installation de boîtes noires chez les FAI ou les hébergeurs et éditeurs pour détecter des comportements suspects d'anonymes, avant de permettre une identification des personnes dont il est confirmé qu'elles méritent une attention particulière.
En Israël, le ratio serait d'environ 20 000 personnes considérées suspectes pour 1 million d'internautes, sur lesquelles ressortiraient entre 10 et 15 profils nécessitant une surveillance étroite.

CHRISTIAN ESTROSI DÉJÀ INTÉRESSÉ

L'information de Reuters confirme ce qu'indiquaient Les Échos le week-end dernier dans un reportage bien informé. « L'Etat hébreu, dont la population a connu sept guerres et deux Intifada depuis sa création, est bel est bien devenu un cas d'école, dans sa façon de gérer une situation d'insécurité permanente. Une expertise dans la mire des décideurs européens », écrivait le quotidien,
Il précisait qu'en février dernier, l'ancien maire de Nice et actuel président de la région Provence-Alpes-Côte d'Azur, Christian Estrosi, s'était déjà rendu en Israël, où il aurait rencontré le PDG de la société Eagle Security and Defense, Giora Eiland, qui est aussi ex-directeur du Conseil de sécurité nationale israélien.
Lors de cette visite, Christian Estrosi aurait insisté sur la nécessité « d'être à la pointe de la lutte par le renseignement contre la cybercriminalité lorsqu'on sait que la radicalisation se fait par le biais des réseaux sociaux ». On imagine que cette conversation lui est revenue en mémoire lorsque sa ville a été meurtrie.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Détecter les futurs terroristes sur Internet ? LEurope veut sinspirer dIsraël – Politique – Numerama

---

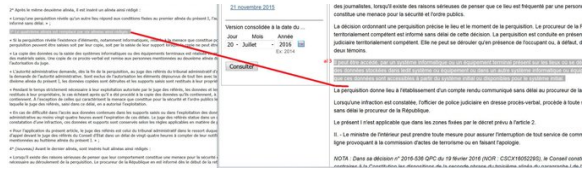
État d’urgence : la police pourra bien copier des données trouvées dans le Cloud

État d’urgence : la police pourra bien copier des données trouvées dans le Cloud

---

Contrairement à ce que nous écrivions mardi avec étonnement, il sera bien possible pour la police d'utiliser l'ordinateur ou le smartphone d'un suspect pour accéder à tous ses services en ligne, puis de copier les informations obtenues pour les exploiter si elles sont pertinentes.

Il faudrait toujours retourner son clavier sept fois sur le bureau avant de donner un satisfecit au gouvernement. Mardi, nous détaillions le cadre prévu dans le projet de loi de prorogation de l'état d'urgence, pour la copie des données informatiques dont Manuel Valls avait annoncé le retour. Il fallait vérifier si les exigences du Conseil constitutionnel en matière de respect de la vie privée étaient bien respectées.
À cette occasion, nous faisions remarquer à tort que le gouvernement n'avait pas prévu la possibilité de copier des données stockées dans les services en ligne des suspects, se limitant curieusement aux seules « *données contenues dans tout système informatique présent sur les lieux de la perquisition* ».
Pris dans un élan de naïveté, nous n'avions pas fait attention au fait que l'ensemble du dispositif n'était pas réécrit, et que le gouvernement avait laissé intacte une disposition non censurée par le Conseil constitutionnel, qui change toute l'analyse. Elle dit qu'en cas de perquisition administrative, « *il peut être accédé, par un système informatique ou un équipement terminal présent sur les lieux où se déroule la perquisition, à des données stockées dans ledit système ou équipement ou dans un autre système informatique ou équipement terminal, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial* ». Créé en novembre 2015, cet alinéa de l'article 11 de la loi du 3 avril 1955 relative à l'état d'urgence n'a pas été supprimé, comme le fait justement remarquer Marc Rees deNext Inpact :
Voir l'image sur Twitter



Suivre

marc rees @reesmarc
. @p_estienne j'ajoute que PJL #EtatdUrgence ne supprime pas accès au cloud cc @gchampeau (gauche PJL droite, L55)
11:03 – 20 Juil 2016
•
•
77 Retweets
•
1 j'aime
Il reste donc possible pour la police d'accéder sur place à toutes données disponibles sur le Cloud, en profitant des sessions ouvertes sur des services en ligne (ou dont le mot de passe est mémorisé). Dès lors, à partir du moment où ils sont affichés à l'écran ou téléchargés, ces messages Facebook, e-mails, documents Google Docs, historiques WhatsApp ou autres fichiers stockés à distance deviennent bien des « *données contenues dans tout système informatique présent sur les lieux de la perquisition* », qui peuvent être copiées et analysées après autorisation du juge, dans le cadre désormais fixé.
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 : État d'urgence : la police pourra bien copier des données trouvées dans le Cloud – Politique – Numerama

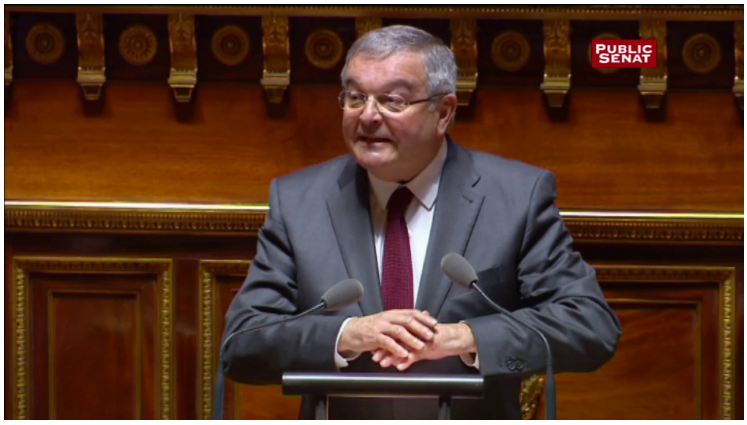
Quelles sont les limites d’accès aux données de connexion en situation d’État d’urgence ?

Quelles sont les limites d’accès aux données de connexion en situation d’État d’urgence ?

Mercredi, le Sénat examinera le projet de loi de prorogation de l'état d'urgence, et discutera à cette occasion d'un amendement qui vise à donner à la police le pouvoir d'obtenir en temps réel les données de connexion de tout suspect de terrorisme, sans aucun contrôle même administratif.

Au nom du comité de suivi de l'état d'urgence dont il est le rapporteur spécial, le sénateur Michel Mercier (UDI-UC) a présenté mardi la substance des amendements qu'il entend présenter devant la commission des lois ce mercredi, pour compléter le projet de loi de prorogation de l'état d'urgence déposé par le gouvernement. Ces amendements ont de fortes chances d'être adoptés par la majorité de droite du Sénat.

Parmi eux, M. Mercier explique qu'un « *amendement aura pour objet de remédier aux rigidités et lourdeurs dans la mise en œuvre de la technique de recueil de renseignements, créée par la loi du 24 juillet 2015, permettant de recueillir en temps réel, sur les réseaux des opérateurs de communications électroniques, les données de connexion relatives à une personne préalablement identifiée comme présentant une menace terroriste* ».



Il s'agit de la procédure créée par la loi Renseignement et codifiée à l'article L851-2 du code de la sécurité intérieure, qui permet « *pour les seuls besoins de la prévention du terrorisme* » d'autoriser « *le recueil en temps réel* » des « *informations ou documents* » détenus par les opérateurs télécoms et les hébergeurs « *relatifs à une personne préalablement identifiée comme présentant une menace* ».

C'EST CE CADRE POURTANT DÉJÀ CRITIQUÉ PAR LES DÉFENSEURS DES DROITS FONDAMENTAUX QUE MICHEL MERCIER ESTIME CONSTITUER DES « RIGIDITÉS ET LOURDEURS »

Même s'il y a débat juridique pour savoir jusqu'où vont ces « informations ou documents », et s'ils vont jusqu'au contenu-même des communications (en principe non), il s'agit au minimum de l'ensemble des données de connexion : adresses IP, numéros de téléphones composés, durées et heures des appels, géolocalisation du téléphone mobile, nombre de SMS échangés, avec qui, de quelle longueur, etc. Potentiellement ce sont donc des données très intrusives dans la vie privée des individus, qui permettent de renseigner sur les habitudes, les déplacements et les contacts.

Actuellement, pour avoir accès en temps réel à ces données, les services de renseignement doivent obligatoirement ***obtenir au préalable une autorisation du Premier ministre****, elle-même délivrée après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR). L'avis de la CNCTR doit intervenir dans les 24 heures ou pour les cas les plus complexes, dans les 72 heures. Mais en cas « d'urgence absolue », il est même* ***possible de se passer de l'avis de la CNCTR****.*

Or c'est ce cadre pourtant déjà critiqué par les défenseurs des droits fondamentaux (en raison de l'absence de contrôle d'un juge indépendant) que Michel Mercier estime constituer des « rigidités et lourdeurs » qu'il faudrait supprimer en cas d'état d'urgence.

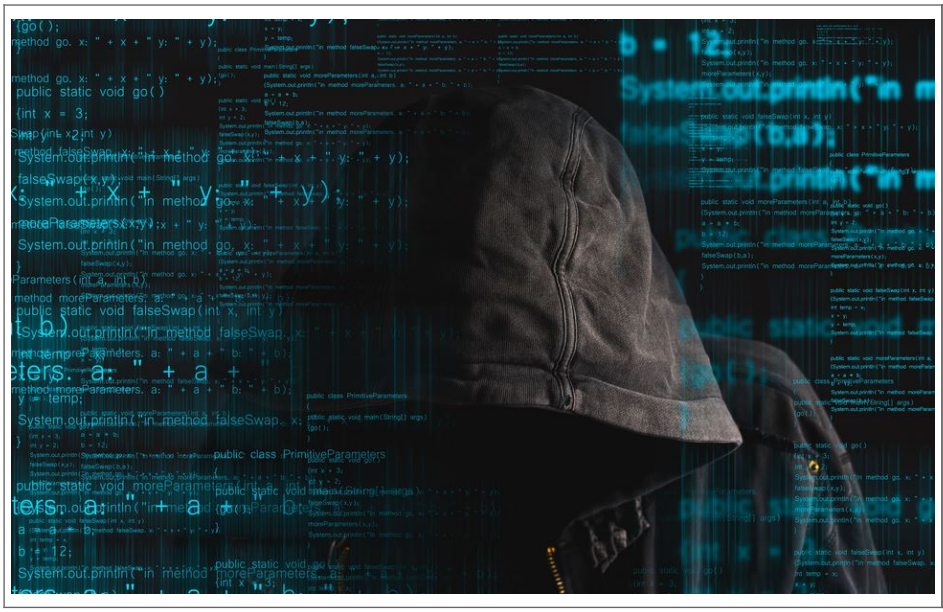
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : État d’urgence : open bar pour la police sur les données de connexion ? – Politique – Numerama

---

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.

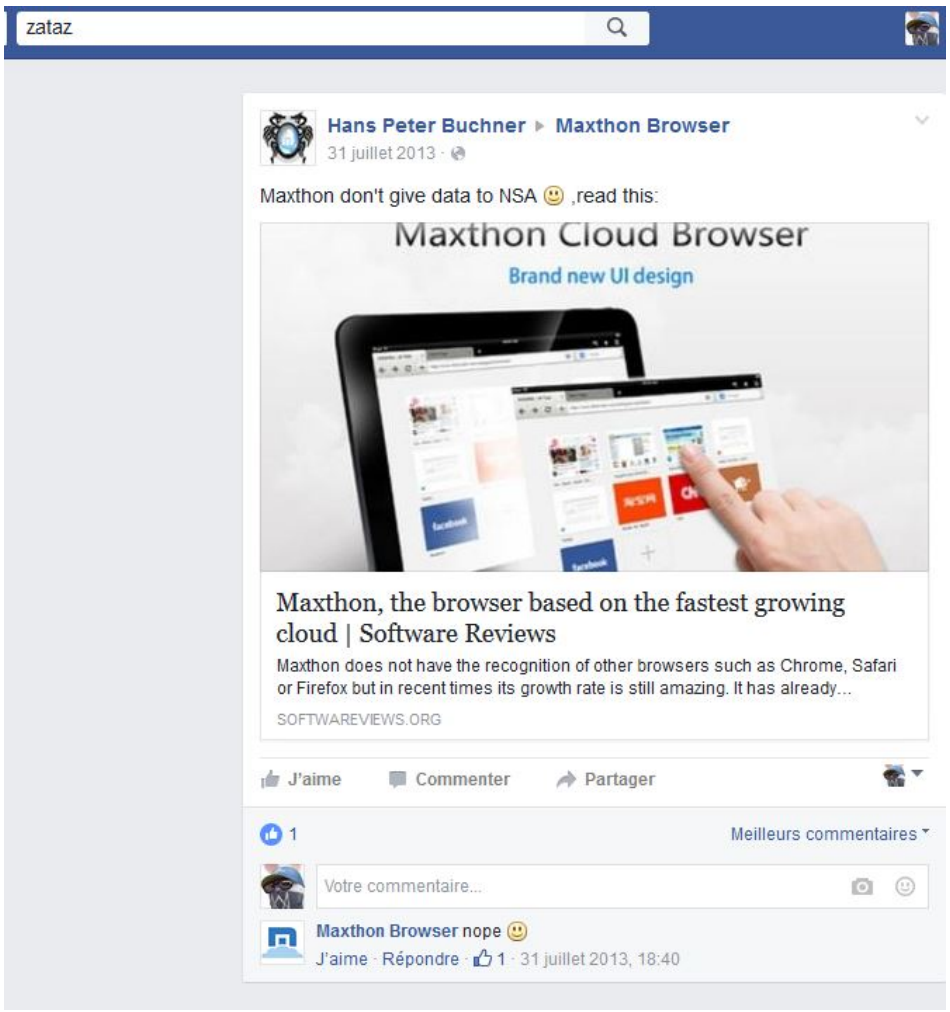
Ce n'est pas la première fois que les entreprises énergétiques sont visées par des malwares ayant pour ambition le sabotage du réseau. On pense bien évidemment au premier virus qui visait les SCADA, Stuxnet. Mais plus récemment, l'Ukraine a été victime d'une panne de courant provoquée par une cyberattaque 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

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

Réagissez à cet article

Original de l'article mis en page : Secret Conversations : Facebook Messenger en mode chiffré