

# [rappel] Les Anonymous s'en prennent au gouvernement français



**Après avoir lancé une attaque par déni de service sur le site du Parti Socialiste hier, les Anonymous semblent aujourd'hui avoir pris pour cible les sites institutionnels du Sénat et de l'Assemblée nationale.**

Les services informatiques de l'Assemblée nationale et du Sénat ont indiqué : « *Nous avons rencontré des problèmes de connexion et sommes en train d'en déterminer l'origine, qui pourrait en effet être une attaque DDoS. En tout cas, cela en a toutes les caractéristiques* ». Attaque ou pas, les auditions habituellement diffusées en direct n'ont pu être retransmises ce matin.

Hier, les Anonymous avait revendiqué une attaque similaire contre le site du Parti socialiste via la publication d'une vidéo sur YouTube. Dans cette dernière, le groupe d'« hacktivistes » fustigeait l'état d'urgence actuellement en cours dans notre pays, regrettant « *l'atteinte à la vie privée que pratique l'Etat français à l'égard de ses citoyens* » qu'il implique.

Une situation autorisée pour cause d'un terrorisme que les Anonymous considèrent comme « *excuse pour nous tromper, pour mieux nous surveiller, nous endormir et nous contrôler* ». Ils avaient hier menacé d'autres actions « *si l'état d'urgence n'est pas rectifié* », rappelant ne vouloir « *aucunement faire de la politique* » et ne viser que « *le site du Parti socialiste car il est le parti du dictateur Hollande.* ». Visiblement, ils auraient changé d'avis.

**Mise à jour :** après les sites du Sénat et celui de l'Assemblée, et après avoir souhaité la bienvenue au nouveau garde des Sceaux, Jean-Jacques Urvoas, en attaquant son blog, les Anonymous s'en sont pris ce matin aux sites des ministères de la Justice et de la Défense.

Si ce dernier est de nouveau sur pied à l'heure où nous écrivons ces lignes, il est toujours impossible de se rendre sur celui du ministère de la Justice. Les choses devraient toutefois revenir en ordre, les Anonymous étant désormais occupés avec les sites gouvernementaux du Burundi, dont la police a arrêté ce matin deux journalistes du *Monde*.



Réagissez à cet article

Source : [rappel] *Les Anonymous s'en prennent au gouvernement français*

---

# Fic 2016 : La sécurisation des objets connectés préoccupe enfin...



Fic 2016 : La  
sécurisation des  
objets  
connectés préoccupe  
enfin...

**Le 8e Forum international de la cybersécurité, qui s'est tenu à Lille les 25 et 26 janvier, a permis de découvrir des solutions qui émergent en France en termes de sécurisation des objets de communication et des systèmes d'information auxquels ils sont connectés. Certaines sont encore à construire comme la plateforme Scop, d'autres sont déjà opérationnelles comme le CERT-Ubik et le boîtier Hardsploit.**

La multiplication des objets communicants, les IoT en anglais pour Internet Of Things, est une excellente opportunité pour la cybercriminalité. Sachant qu'à chacun de ces objets correspond une adresse IP, leur diffusion rend les réseaux très perméables.

*« On estime à plus 50 milliards leur nombre d'ici 2020, soit 7 objets connectés par personne sachant qu'il y aura 7,5 milliards d'habitants sur terre. Les hackers vont pouvoir profiter d'une perméabilité des systèmes d'informations jamais atteintes jusqu'à présent. Et si la sécurité était en réalité le principal enjeu de l'Internet des objets ? »*

*A cette question posée en introduction de son exposé lors du 8e Forum International de la Cybersécurité, Christophe Joly, le directeur sécurité de Cisco France, a bien sûr répondu par l'affirmatif en chiffrant à plus de 375 milliards de dollars le marché annuel du cybercrime qui se profile. Mais comme avec les voitures au début du vingtième siècle et avec Internet plus récemment, le législateur attendra sans doute qu'une catastrophe ait lieu avant de mettre en place des règles. En attendant, rien n'empêche de se protéger.*

## **Sécuriser l'électronique embarquée**

*Pour Cisco, le leader mondial des technologies informatiques de connectivité, les moyens de le faire passent par une bonne connaissance de son infrastructure informatique et des objets qui s'y connectent. Mais cette approche ne suffit pas toujours, entre autres quand l'objet communique par radiofréquence. De plus, la sécurité des objets connectés ne porte pas uniquement sur les réseaux et les... Lire la suite...*



Réagissez à cet article

Source : *Cybercriminalité: la sécurisation des objets connectés est en marche au FIC*

---

# Programme de la 6eme Edition IT Forum à Dakar au Senegal

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
|  <p>En partenariat avec</p>   <p><b>Organise la 6<sup>eme</sup> édition de l'IT Forum Sénégal</b></p> <p>« Enjeux de stratégie nationale pour le secteur numérique en Afrique de l'Ouest. Quelle place pour la cyber-sécurité ? » »</p> <p><b>18 et 19 février 2016 à l'hotel les Almadies, Dakar</b></p> | <p>Programme de la<br/>6eme Edition IT<br/>Forum à Dakar au<br/>Senegal</p> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|

---



**PROGRAMME DU JEUDI 18 FEVRIER 2015**

9h00-9h10 DISCOURS DE BIENVENUE

Par M. Mohamadou DIALLO, Directeur de la publication de Cio Mag

9h10-9h20 ALLOCUTION D'OUVERTURE

Approche nationale et régionale en matière de Cybercriminalité

Par M. Yaya Abdoul KANE, Ministre de la Poste et des Télécommunications

9h20-9h30 ALLOCUTION Pays Invité d'honneur

Lutte contre la cybercriminalité, la Côte d'Ivoire renforce son arsenal

Par M. Bruno N. KONE, Ministre de la Postes et des Technologies de la Communication de Côte d'Ivoire, Porte-parole du Gouvernement

9h30-9h50 KEYNOTE SPEAKER

Pas d'Economie Numérique sans cyber-sécurité : Comment faire face aux tendances du numérique tout en maîtrisant les défis du Cyberespace ?

Par M. Thierry BRETON, Président Directeur Général d'ATOS

9h50-10h00 KEYNOTE SPEAKER

L'Arrivée des réseaux haut débit, un accélérateur ou un moyen efficace de lutter contre les cyberattaques

Session Introductive

9h50-10h30 2 POINTS DE VUE

– Cyber sécurité et protection des données à caractère personnel

Par M. Mouhamadou IO, Président de la Commission de Protection des Données Personnelles (CDP) du Sénégal

– Cybercriminalité : enjeu international

Par M. Ali Drissa BADIOEL, Représentant de l'UIT (Union Internationale des Télécommunications) en Afrique de l'Ouest

Questions / Réponses

10h30-11h00 Pause café et visite des stands

11h00-12h00 Plénière 1

Cloud, Mobilité, big data, internet des objets, Byod : Comment intégrer les nouvelles tendances tout en maîtrisant les nouveaux risques inhérents ?

Moderateur: Commandant Guelpehetchin QUATTARA, Directeur de l'informatique et des Traces Technologiques de Côte d'Ivoire

• Représentant opérateur (Orange/Tigo ou Expresso Télécom)

• M. Chris MORET, Responsable de la Global Business Line CyberSecurity d'Atos Big Data & Secrity

• Dr. Aloune DIONE, Directeur des Systèmes d'Information de la Douane

• Colonel Julien DECHAMET, Officier Cyber des Eléments Français en Afrique de l'Ouest

• M. Jean-Paul PINTE, Expert International en Cybercriminalité,

• Alain DOLLIUM, Co-fondateur et CEO EMEA North America de South Mobile Service,

Questions / Réponses

12h00-13h00 Plénière 2

Plan Numérique et Administration électronique : Quelles perspectives ?

Moderateur : M. Alain DUCASSE, Expert en Transformation Digitale

• Présentation des grandes lignes du Plan stratégique pour le numérique (Côte d'Ivoire/Sénégal) Par M Euloge Kipeya SORO, Directeur Général de l'Agence Nationale du Service Universel des Télécommunications ( ANSUT)

• M. Malick NDIAYE Directeur de Cabinet du Ministère des Poste et des Télécommunications du Sénégal

• M. Mouhamed Tidiane Seck, Directeur Associé Performances Management Consulting

• M. Cheikh BAKHOUM, Directeur Général de l'Agence de l'Informatique de l'Etat (ADIE)

• M. Brice DEMOGE, Directeur du développement Secteur Public et Afrique – GFI Informatique

Questions / Réponses

13h00-14h00

Pause Déjeuner

14h00-15h00 Plénière 3

Retours d'expériences : solutions

• Plan de Sauvegarde et réplication des donnée après un incidents

• SAP s'engage pour la préservation du Parc Nizokolokoba

• Cloud, l'essentiel pour les entreprises

Par Opérateur (Orange/Tigo ou Expresso Télécom)

• Applications métiers en mode Cloud, GFI informatique / Cegid

– Big data et sécurité, M. Alain DOLLIUM, CEO South Mobile Services

Questions / Réponses

15h00-16h00 Plénière 4

Quelles solutions face à l'internationalisation de la cybercriminalité ?

• Moderateur : M. Papa Assane TOURE, Magistrat, Secrétaire général adjoint du Gouvernement

• M. Pape GUEYE, Elève Commissaire de Police, Ancien Chef de la Brigade de lutte contre la cybercriminalité

• M. Jean-François BEUZE, Président Directeur Général de Sifaris

• M. Ali El AZZOUI, Président Directeur Général Data Protect

• M. Richard NOUNI, Directeur Général de CFAO Technologies

• Retour d'expériences du secteur bancaire

Questions / Réponses

16h00-16h30

Pause café et visite des stands

16h30-17h30 Plénière 5

Point d'Echange Internet et ouverture du marché des FAI : Vers une amélioration de la qualité de l'Internet au Sénégal ?

Moderateur : M. Mohamadou SAIBOU, Directeur de l'ESMT Dakar

• M. Cheikh BAKHOUM, Président de SENIX (Point d'Echange Sénégal)

• M. Tidiane DEME, Google Afrique

• M. Ali Drissa BADIOEL, Représentant de l'UIT (Union Internationale des Télécommunications) en Afrique de l'Ouest

• M. Alex CORENTIN, Président d'ISOC Sénégal

• Représentant de l'ARTP

Questions / Réponses

17h30-17h45

SDE/Sodeci (Société d'électricité et d'eau de Côte d'Ivoire) face aux enjeux de l'électronique

SEM Sylvestre, Directeur Général de GSZE (Groupement d'intérêt économique de CIE et SODECI).

Clôture

17h45-18h00

DISCOURS DE CLÔTURE

Perspectives sur les enjeux du haut débit mobile au Sénégal avec l'arrivée de la 4G

Par M. Yaya Abdoul KANE, Ministre de la Poste et des Télécommunications

**PRE-PROGRAMME DU VENDREDI 19 FEVRIER 2015**

Réflexion sur les chantiers de Modernisation de l'administration publique – Trois cas

9h00-9h15 Ouverture

DISCOURS D'OUVERTURE

Par M. Alioune SARR, Ministre du Commerce, du Secteur informel, de la Consommation, de la Promotion des produits locaux et des PME du Sénégal

9h15-10h00 Plénière 1

CAS 1 – SIGIF (Système Intégré de Gestion des Informations financières)

Le SIGIF, un enjeu de modernisation et de transparence dans la gestion des comptes publics

• Gestion Intégrée des finances publiques : Retour d'expériences de la Côte d'Ivoire

Par Nongolougo SORO, Directeur Général de la SNOI

• Direction Générale de la comptabilité publique et du Trésor

• M. Ibrahim FAYE, Chef de l'Equipe Projet SIGIF au Ministère de l'Economie des Finances et du Plan

• M. Frédéric MASSE, VP SAP

• M. Jean-Michel HUET, Associé BearingPoint

Questions / Réponses

10h00-11h00 Plénière 2

CAS 2 – GUICHET UNIQUE

Guichet unique et impact sur le Doing business

• Directeur du commerce au Ministère du commerce

• Ibrahim DIAGNE, DG de Gainé 2000

• Représentant de l'Apix

• Dr. Alioune DIONE, DSI de la Douane Sénégalaise

Questions / Réponses

11h00-11h20

Pause café et visite des stands

11h20-12h00 Plénière 3

CAS 3 – FICHER D'ETAT CIVIL

Modernisation du Fichier d'état civil, quel enjeu pour la gouvernance locale ?

Moderateur: André GRISSOMANACHE, PG Exense

– M. Frédéric Massé, VP SAP,

– Mme Emilie Scallier, Gdexpert

– M. Mouhamed Tidiane Seck, Directeur Associé Performances Management Consulting

– Jean-Pierre La Housse de La Louvière, CEO d'ISTEC

– ADIE

– Ministère de l'Intérieur

– Direction de l'état civil

Clôture

12h00-12h20

DISCOURS DE CLÔTURE

Par M. Abdoulaye Diouf SARR, Ministre de la gouvernance locale, du développement et de l'aménagement du territoire du Sénégal

12h20

Cocktail déjeunatoire



Réagissez à cet article

Source : *Programme 6eme Edition IT Forum Senegal – Colloque, Rencontre, IT Forum pour les managers IT africains*

---

## **Fic 2016 : Orange a de grands projets pour la France**



**Une introduction calibrée sur mesure pour Stéphane Richard, PDG d'Orange, qui a succédé à Xavier Bertrand et au général Favier, directeur général de la Gendarmerie Nationale, sur la scène du FIC.**

Lundi 25 janvier 2016, au FIC (Forum International de la Cybersecurité) à Lille Grand Palais

« La politique de cybersécurité d'Orange a été boostée par des attaques et nous peinons à recruter des talents.

2600 postes sont aujourd'hui ouverts à Paris pour la cyberdéfense et il est difficile de les pourvoir.

Notre cyber SOC (security operation center) est installé à Rennes mais nous allons également nous positionner à Lille pour déployer des ressources capables de se projeter à Lille, Bruxelles et Paris », a assuré le PDG.

« Notre croissance – près de 20% par an – est aujourd'hui freinée car nous manquons de ressources », a ajouté Michel van den Bergue, directeur d'Orange Cyberdéfense. « Il est rageant de voir ce domaine avec une perspective énorme manquer de ressources ». Pour Lille, Orange va s'appuyer sur Euratechnologies et travailler avec le personnel de la compagnie qui désire évoluer vers les métiers de la cybersécurité pour répondre à des projets sur Paris, Londres et Bruxelles.



Réagissez à cet article

**Ils notifient une faille sur  
un site web puis reçoivent la  
visite des gendarmes**



Ils  
notifient  
une faille  
sur un  
site web  
puis  
reçoivent  
la visite  
des  
gendarmes

**Deux entrepreneurs se retrouvent en garde en vue après avoir trouvé une vulnérabilité dans le site de Forum international de la cybercriminalité (FIC). Ce dernier, en effet, a porté plainte pour accès frauduleux dans un système informatique.**

Attention, le métier de chercheur en sécurité n'est pas totalement sans risque, comme viennent de le constater deux jeunes entrepreneurs qui viennent tout juste de créer Cesar Security, une société spécialisée dans les audits de sécurité et la prévention contre la fraude bancaire.

La semaine dernière, ils trouvent une faille sur le site web du Forum International de Cybersécurité (FIC) qui se déroule ce jour à Lille.

Selon eux, la vulnérabilité – désormais corrigée – était assez banale, mais permettait quand même d'accéder à la base de données des participants. Pas terrible pour l'image de marque d'un tel événement qui accueille chaque année le gratin français en matière de cybersécurité. Les deux hommes veulent faire les choses bien et contactent l'éditeur du site, à savoir la Compagnie Européenne d'Intelligence Stratégique (CEIS), co-organisateur de l'évènement. Parallèlement, ils envoient une alerte sur Twitter.

Ils sont aimablement reçus au téléphone par un consultant en sécurité du CEIS auprès de qui ils détaillent leur trouvaille. Ils lui envoient un rapport technique de la faille avec une proposition de correctif, un accord de confidentialité ainsi qu'un devis pour un audit de sécurité. « Au départ, nous lui avons proposé un audit gratuit, mais il a dit que ce n'était pas un problème, que l'on pouvait lui envoyer un devis chiffré », nous explique S. Oukas, l'un des deux entrepreneurs. Puis, c'est le silence radio, plus aucune nouvelle. Le 20 janvier, ils envoient donc un nouveau tweet, pour « prendre des nouvelles ».



© DR

Le jour suivant, c'est la surprise. A 9h du matin, les gendarmes sur Centre de lutte contre les cybercriminalités numériques (C3N) toquent à leur porte. Ils apprennent que l'éditeur du site a porté plainte pour « accès frauduleux à un système de traitement automatisé de données » (STAD), un délit passible de deux ans d'emprisonnement et d'une amende de 60 000 euros.

Tout le matériel informatique est saisi. « Nous avons tout perdu : les trois ordinateurs dans notre bureau, un téléphone, un ordinateur personnel et même une PlayStation. Nous sommes tombés de très haut. Nous qui pensions que le FIC aurait encouragé une jeune startup, ils nous mettent à genou. Nous avons perdu nos outils de travail, nous ne pouvons plus rien faire », souligne M. Oukas.

### **Vente forcée ou chevalier blanc ?**

De son côté, le CEIS n'a pas la même interprétation des choses. « Cette société nous a bien contactés, mais ce n'était pas désintéressé car elle nous a proposé ses services. Nous ne l'avons jamais autorisé à effectuer cette recherche. C'est de l'audit sauvage », estime Guillaume Tissier, directeur général du CEIS, qui n'a pas apprécié non plus que Cesar Security publie son alerte de sécurité de manière publique sur Twitter, aux yeux de tous. « Au tribunal, le débat tournera certainement autour de cette question, car on peut le voir comme une forme de vente forcée », estime pour sa part Bernard Lamon, avocat.

L'ironie du sort, c'est que cette affaire tombe pile au moment où les députés votent un amendement visant à protéger les lanceurs d'alerte qui trouvent des failles informatiques. Selon le texte, une telle personne sera exempte de peine « si elle a immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système ». Ce texte, s'il est adopté au final, pourrait néanmoins jouer en faveur de Cesar Security. « Même si les faits sont antérieurs, le texte sera applicable car il est plus clément », souligne Bernard Lamon.



Réagissez à cet article

**Source : Ils notifient une faille sur un site web puis reçoivent la visite des gendarmes**

---

# D'où vient le danger des Objets connectés ?



D'où  
vient le  
danger  
des  
Objets  
connectés  
?

**Le développement des objets connectés s'accélère de plus en plus tandis que la mise en place de moyens de sécurité reste quant à elle beaucoup plus discrète... Tout le monde connaît le récit mythique du cheval de Troie, alors ne sommes-nous pas en train de danser sur ce qui va causer la perte de notre identité à chacun ? Qu'en est-il des normes de sécurité dans le domaine des objets connectés ? Comment pouvons-nous protéger nos données personnelles ?**

Deux étudiants en médecine, ont pointé du doigt les failles que pourraient comporter certains objets connectés, dans des actions spectaculaires : prendre le contrôle d'un Pacemaker à distance ou encore désactiver les freins d'une voiture connectée. Ces actions coups de poing mettent à nu les faiblesses que comportent certains objets connectés face à des hackers malveillants. En effet, c'est précisément là que se situe le paradoxe des nouvelles technologies qu'utilisent les objets connectés... Car s'ils sont conçus pour nous faciliter le quotidien, ils peuvent au contraire nous faire beaucoup de mal et en particulier à nos données personnelles ! Pour pouvoir se protéger, il faut avant tout comprendre cette technologie et adopter quelques habitudes très utiles.

#### **Tout objet connecté peut être hacké**

Pour comprendre comment une balance connectée peut devenir notre ennemi numéro 1, il faut d'abord comprendre comment cheminent des data (c'est-à-dire les données personnelles qui sont recueillies pendant l'utilisation de l'objet connecté) vous concernant, quels en sont les tenants et les aboutissants et où sont stockés ces données.

Il existe trois principaux canaux par lesquels voyagent nos data : les réseaux Wifi, le Bluetooth et les réseaux cellulaires pour objets connectés (Sigfox et Lora sont deux des principaux acteurs de ces réseaux).

Ces données sont ensuite acheminées jusqu'aux serveurs du fabricant ou du développeur de l'application pour ensuite revenir vers vous avant de repartir sur le Cloud... Au milieu de tous ces voyages, il devient très facile de voler ou de prendre le contrôle de vos objets, surtout si vous passez par un réseau public.

#### **Le hackage est une menace très sérieuse à prendre en compte**

En 2015, on a constaté une augmentation de 50 % de la cyber-criminalité en France ! Les concepteurs et développeurs d'objets connectés nous parlent sans cesse de nouveautés incroyables et parfaites pourtant comment celles-ci sont-elles sécurisées ? Est-ce que les différents fournisseurs appliquent ou suivent des normes ou une réglementation officielle pour sécuriser le matériel de fabrication ? Il semble qu'il n'y ait pas encore de législation officielle qui soit mise en place, même si la CNIL (Commission Nationale de l'Informatique et des libertés) s'est dernièrement attelé au sujet lors du Forum International de la cyber-sécurité.

#### **Sécurité des objets connectés**

C'est lors des voyages des data que celles-ci sont les plus vulnérables.

Mais le problème reste entier tant que les données qui voyagent ne seront pas cryptées... Ces données personnelles récoltées par les objets connectés peuvent avoir un intérêt économique pour certaines sociétés.

Ainsi, votre balance connectée peut en dire long sur vos habitudes alimentaires, votre traqueur de sommeil connecté peut donner, lui aussi, de précieuses informations sur vos habitudes de vie quotidienne. Ces données qui peuvent se monnayer très cher favorisent le profilage ciblé pour les publicités notamment et vous enlever petit à petit la liberté d'acheter ce qui vous plaît et non pas ce que l'on vous a suggéré. Le reste des data qui vous concerne, comme vos données bancaires ne sont, également, pas à l'abri d'un hacker qui chercherait à vous voler de l'argent sans toucher à votre porte-monnaie !

#### **Optimisez la sécurité de vos objets connectés**

Face aux deux risques majeurs de la reprise malveillante de vos données personnelles : l'utilisation commerciale et le piratage des données personnelles, vous pouvez adopter quelques gestes simples pour augmenter la sécurité de vos data. Si les objets connectés s'avèrent être dans de nombreux cas, un formidable assistant dans la vie quotidienne pour surveiller votre alimentation, votre sommeil, ... Au contraire, s'ils sont mal connus ou utilisés d'une mauvaise manière, ils peuvent devenir très dangereux pour le particulier. Vous ne devez pas oublier qu'il est essentiel de comprendre comment fonctionnent ces technologies pour en profiter au maximum sans crainte.

Dans un premier temps, vous devez lister tous les objets connectés en activité dans votre maison et déterminer pour chacun d'entre-eux à quoi ils sont connectés et par quel biais (Wifi ou Bluetooth ou réseau cellulaire). Par cet inventaire un peu minutieux mais très utile, vous pourrez contrôler le cheminement de vos données personnelles et savoir quel objet connecté communique par des biais peu sécurisés. Pour que votre sécurité soit optimale, vous devez également effectuer régulièrement des mises à jour en ce qui concerne la sécurité et surtout changer régulièrement les mots de passe et vos identifiants. Il ne faut pas oublier que même si vos objets connectés restent dans votre maison, les data qu'ils produisent voyagent eux sur le net et donc dans le monde !



Réagissez à cet article

**Source : IOT et sécurité : ne laissez plus le cheval de Troie entrer chez vous**

---

# Une Vauclusienne se fait escroquer de 23000 euros par téléphone



Une  
Vauclusienne  
se fait  
escroquer de  
23000 euros  
par  
téléphone

## **Difficile de faire plus simple comme escroquerie : une fausse avocate a escroqué une habitante du Vaucluse de près de 23000 euros par de simples appels téléphoniques**

En décembre dernier, la faussaire appelle cette habitante de Saint-Romain en Viennois, près de Vaison-la-Romaine, qui vient de perdre son père, pour lui annoncer qu'il avait contracté une assurance-vie à son bénéfice.

Pour toucher les 127 000 euros de capital, elle doit d'abord payer 9500 euros d'honoraires. Elle s'exécute, après avoir reçu des documents convaincants par mail, et fait un virement... en Lituanie. Quelques jours plus tard, rebelote, cette fois avec un virement de près de 13500 euros en Bulgarie. «Il lui faudra encore quelques jours pour se douter d'une entourloupe.

Elle s'adresse alors à sa banque, qui lui confirme qu'elle a été escroquée», raconte le journal. Un stratagème simple, qui rappelle «l'arnaque au PDG», dont sont victimes depuis plusieurs années de nombreuses entreprises françaises.



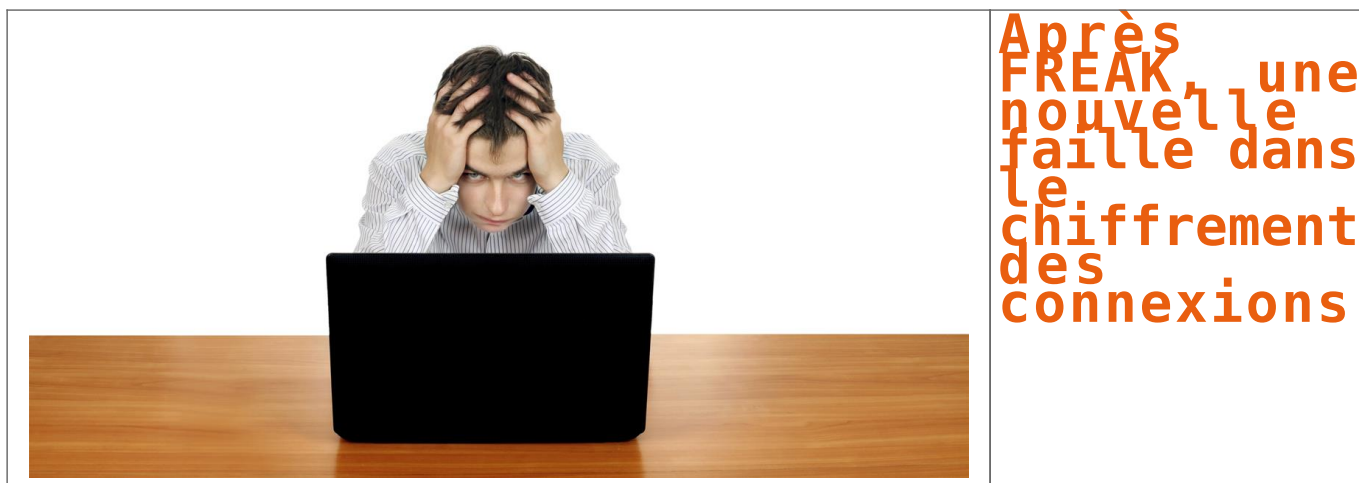
Réagissez à cet article

Source : *Une Vauclusienne se fait escroquer de 23000 euros par téléphone*

---

# **Après FREAK, une nouvelle**

# faille dans le chiffrement des connexions



Une nouvelle faille de sécurité vient de remonter à la surface : #Logjam. Né des cendres de FREAK, elle reprend le même principe de fonctionnement et permet d'établir une connexion chiffrée avec une clé trop petite pour être réellement efficace.

Au début du mois de mars, la #faille FREAK secouait Internet, pour plusieurs raisons. Tout d'abord, car elle permettait (et permet toujours) d'intercepter des échanges de données chiffrés entre un serveur et un navigateur. Ensuite car il s'agissait d'un reliquat des années 90 lorsque les États-Unis limitaient l'exportation des systèmes de chiffrements à 512 bits maximum (voir cette actualité pour plus de détail). Bien évidemment, bon nombre de serveurs et de navigateurs avaient été rapidement mis à jour suite à cette découverte.

Il convient néanmoins de relativiser puisqu'il faut procéder à une attaque de type « homme du milieu » pour l'exploiter, et donc être sur le même réseau (un « hot-spot » Wi-Fi par exemple), ce qui n'est pas toujours des plus pratiques. On est loin de la portée de Heartbleed par exemple, qui permettait à n'importe qui de lire des données directement dans la mémoire d'un serveur (identifiant, mot de passe, carte bancaire, etc.).

### De FREAK à Logjam, toujours la même histoire de chiffrement « faible »

Mais une faille peut en cacher une autre et voilà désormais qu'il est question de Logjam. Elle est détaillée dans ce document, signé par des chercheurs de l'INRIA de Paris et de Nancy, de l'université de Pennsylvanie, de Johns Hopkins, du Michigan et de chez Microsoft Research. Selon les chercheurs, « cette attaque rappelle FREAK, mais elle est due à une faille dans le protocole TLS plutôt qu'à une vulnérabilité dans son implémentation, et elle cible un échange de clés Diffie-Hellman plutôt que d'un échange de clés RSA ».

Avec la faille FREAK et l'utilisation de la fonction « export RSA », un serveur répond avec une clé RSA de 512 bits, tandis qu'avec Logjam et « DHE\_EXPORT », serveur et navigateur procèdent à un échange de clés via le protocole Diffie-Hellman, mais dans des groupes de 512 bits seulement... ce qui n'est pas suffisant pour résister à une attaque. On notera que ce problème avait déjà été évoqué par certains il y a plusieurs mois. La situation n'est donc pas nouvelle, mais elle prend une autre tournure.

### Serveurs et navigateurs doivent se mettre à jour

Là encore, le problème concerne les navigateurs et les serveurs : il suffit que l'un des deux n'accepte pas un groupe de 512 bits pour que l'attaque échoue. De plus, et comme avec FREAK, il faut être sur le même réseau pour que cela fonctionne via une attaque de l'homme du milieu, ce qui limite évidemment la portée, mais n'enlève rien à sa dangerosité.

Du côté des navigateurs, Internet Explorer ne semble pas vulnérable si l'on en croit l'outil de test proposé par le site WeakDH.org, mais Chrome et Firefox le sont. Adam Langley, un cryptanalyste qui travaille chez Google, s'est exprimé sur le sujet sur l'un des forums du géant du web : « *En se basant sur leur travail, nous avons désactivé TLS False-Start avec Diffie-Hellman dans Chrome 42, qui est la version stable depuis plusieurs semaines maintenant* [NDLR : on est passé à Chrome 43 depuis ce matin, mais cela ne change rien sur le principe]. Cette attaque sur les serveurs vulnérables sera un peu plus difficile ».

#### The Logjam Attack

Warning! Your web browser is vulnerable to Logjam and can be tricked into using weak encryption. You should update your browser.

### Passer à 1 024 bits minimum, voire mieux à Diffie-Hellman sur des courbes elliptiques

Pour autant, cela n'est pas encore suffisant et Adam Langley ajoute que « le tronc commun du code de Chrome changera afin d'imposer une nouvelle taille de 1024 bits pour Diffie-Hellman. Même si cela entraînera des problèmes pour certains sites, le travail d'aujourd'hui montre que nous ne devrions pas considérer de tels sites comme sécurisés de toute manière ». Il précise que « ce changement est en bonne voie d'être inclus dans Chrome 45 », mais que le calendrier pourrait être plus rapide.

Mais tout cela ne sera probablement qu'une solution temporaire. En effet, les chercheurs à l'origine de la publication de Logjam indiquent qu'un groupe de 1 024 bits peut être « cassé » par un pays ayant suffisamment de moyens (on pense notamment à la NSA qui décrypte à tout-va), et cela ne fera qu'empirer avec le temps. Le cryptographe de Google rejoint cette conclusion : « *Un minimum de 1024 bits ne suffit pas sur le long terme. Malheureusement, parce que certains clients ne prennent pas en charge les groupes de DH supérieurs à 1024 bits, et parce que TLS ne négocie pas spécifiquement certains groupes, il serait très problématique de pousser cette limite au-dessus de 1024. Alors que nous approchons de l'élimination du chiffrement RSA sur 1024 bits, nous nous interrogeons de manière plus générale sur la prise en charge des groupes non elliptiques DHE dans TLS* ». Cela laisse entendre que cette méthode pourrait disparaître à terme, en tout cas chez Google.

Il existe en effet une version plus sécurisée de ce protocole : ECDHE pour Elliptic curve Diffie-Hellman (ou bien encore Diffie-Hellman sur des courbes elliptiques). Pour Google, « les serveurs qui utilisent actuellement DHE devraient se mettre à jour et passer à ECDHE. Si cela est impossible, utilisez au moins DHE avec des groupes de 1024 bits et ne soyez pas trop surpris si Chrome commence à utiliser du chiffrement RSA avec votre site dans le futur ».

### Un guide des bonnes pratiques et un site pour tester navigateurs et serveurs

Cette recommandation est d'ailleurs également faite par l'équipe de chercheurs qui a mis en ligne un petit guide du déploiement de Diffie-Hellman, ainsi qu'un outil de test. Il recommande de désactiver les fonctions Export Cipher Suites, déployer un système de Diffie-Hellman sur des courbes elliptiques et utiliser un groupe fort et unique pour chaque serveur.

Comme toujours, on devrait voir arriver une série de correctifs dans les prochaines semaines, à la fois côté navigateur et serveur. Cela ne devrait pas tarder puisque les principaux concernés ont été mis au courant avant que la faille ne soit rendue publique.



Réagissez à cet article

Source : Logjam : après FREAK, une nouvelle faille dans le chiffrement des connexions – Next INpact

---

# Le chaos à la suite d'une attaque informatique ? C'est théoriquement possible



**L'experte en cybersécurité Solange Ghernaouti évoque l'association des actes de terrorisme classique avec le cyberterrorisme. Elle explique comment des outils de communications peuvent déstabiliser la population.**



Invitée du Journal du Matin à l'occasion de la « Journée stratégique 2016 » de l'Association suisse de la sécurité de l'information (Clusis), Solange Ghernaouti explique de quelle manière des systèmes informatiques complexes peuvent déstabiliser le monde réel. Surtout lorsqu'ils tombent dans de mauvaises mains, comme celles de terroristes.

« Le groupe Etat islamique est en train de monter en puissance dans ce domaine. Ils sont très forts dans l'usage de l'internet, notamment dans la communication. » La spécialiste en cybersécurité à l'Université de Lausanne cite l'exemple d'applications sur android pour téléphones portables, développés par l'EI pour communiquer de manière sécurisée.

### **« Cologne était délibéré »**

Selon elle, les agressions sexuelles de Cologne étaient d'ailleurs organisées et aidées par des outils de communication sophistiqués. « Le viol est une arme de guerre », rappelle-t-elle. Or, ces événements étaient une volonté délibérée de déstabiliser la population.

« Nous n'avons pas encore pris la mesure de ce que pouvaient faire les outils de communication pour donner du pouvoir à des terroristes », souligne-t-elle.

### **Attaquer de gros ouvrages**

Au-delà des outils de communication, Solange Ghernaouti évoque aussi les attaques informatiques sur des infrastructures critiques. « Le chaos est théoriquement possible », affirme-t-elle. Par exemple, la Suisse pourrait être privée d'électricité durant plusieurs jours.

Il est également possible, explique-t-elle, de prendre le contrôle des systèmes qui gèrent des barrages, pouvant engendrer des catastrophes naturelles. Pire: en manipulant des données informatiques servant à réguler la qualité de l'eau, il est possible d'infecter des réseaux de distribution.

« Le groupe Etat islamique n'a pas encore les moyens de pirater de grands ouvrages, mais c'est l'étape d'après », alerte Solange Ghernaouti.

### **Sous-effectifs en Suisse**

Si la Confédération a déjà pris conscience des risques et des menaces informatiques possibles, le problème se situe ailleurs, estime-t-elle. « Il y a un décalage entre le conceptuel et les moyens à dégager pour mettre ces risques sous contrôle. »

L'effectif de la cyberdéfense en Suisse se compterait sur les doigts d'une main, selon l'experte, qui appelle le nouveau conseiller fédéral Guy Parmelin à « porter ce débat au niveau le plus haut du pays ».



Réagissez à cet article

Source : « Avec une attaque informatique, le chaos est théoriquement possible » – rts.ch – Suisse

---

# La boîte à outils des gendarmes du Net pour lutter contre la Cybercriminalité



La boîte à outils  
des gendarmes du  
Net pour lutter  
contre  
la Cybercriminalité

**Installé au sein du pôle judiciaire de la gendarmerie nationale à Cergy-Pontoise, le centre de lutte contre les criminalités numériques (C3N) utilise une palette d'outils pour patrouiller sur le web et détecter toutes sortes d'infractions en ligne.**

Depuis un an, l'unité lutte de manière active contre la propagande djihadiste et l'apologie du terrorisme. Elle s'est dotée pour cela de nouveaux outils et a renforcé ses équipes.

« *Nous sommes un peu la Bac du net. Notre travail consiste à patrouiller sur Internet pour détecter des infractions* », explique le colonel de gendarmerie **Nicolas Duvinage**, chef du centre de lutte contre les criminalités numériques. Cette entité, baptisée le **C3N**, rassemble 35 militaires. Elle est installée au Pôle judiciaire de la gendarmerie nationale (**PJGN**), dont les nouveaux locaux se situent à Cergy-Pontoise (Val d'Oise).

Le C3N mène trois principales missions : il anime et coordonne le réseau **CyberGend**, déployé sur tout le territoire, effectue du renseignement criminel (pour réaliser une cartographie et une typologie des auteurs et des victimes et détecter les modes opératoires émergents) et réalise des enquêtes judiciaires pour détecter les fameuses infractions commises en ligne. Dans le cadre de cette mission, les gendarmes interviennent dans plusieurs cas : pour les atteintes aux stades (attaques informatiques), les atteintes aux biens (contrefaçon), et les atteintes aux personnes (porno-pédographie). « *Depuis janvier 2015, nous participons également de manière active à la lutte contre la propagande djihadiste et l'apologie du terrorisme. Nous nous inscrivons dans une activité plus pérenne dans ce domaine* », confie le colonel Nicolas Duvinage, avant de poursuivre : « *Le but n'est pas simplement de fermer un site ou de retirer des tweets, mais d'identifier les auteurs des tweets et de les interpeller pour les juger* ».

#### **OsintLab pour patrouiller sur Twitter**

35 personnes pour patrouiller sur la toile cela fait peu... Les équipes se sont donc équipées d'une palette d'outils de surveillance automatique ou semi-automatique. Un investissement logiciel qui représente plusieurs centaines de milliers d'euros par an. Parmi ces outils, le logiciel **OsintLab** développé par **Thales** et acheté en 2015. Celui-ci permet de sillonner **Twitter** en s'appuyant sur des mots clefs. « *Cet outil nous a permis de mener plusieurs dizaines d'enquêtes judiciaires au travers desquelles nous avons pu identifier des personnes radicalisées* », assure le colonel. Après avoir « logé » ces personnes, les équipes du C3N transfèrent le dossier à l'échelon spécialisé ou l'échelon territorial compétent, qui se chargera de réaliser l'interpellation.

#### **Advestisearch pour identifier les primo-diffuseurs**

Le C3N utilise également le logiciel **Advestisearch** d'**Hologram Industries**, qui permet de rechercher et d'identifier des contenus illégaux et illicites sous forme de texte, d'image ou de vidéo. « *Grâce à une image fournie en entrée, nous pouvons trouver en sortie des images similaires. Par exemple, lorsqu'une équipe de gendarmes récupère une vidéo de 10 secondes, l'outil nous permet de retrouver la vidéo complète. Cela nous permet aussi de détecter les primo-diffuseurs* », détaille le colonel.

#### **Et bientôt un Scraper Deep Web maison**

Le C3N n'utilise pas uniquement des logiciels « sur étagère », mais développe également ses propres outils. L'unité s'attèle, par exemple, à mettre au point son propre **Scraper Deep Web**, un outil qui permet de collecter automatiquement des petits morceaux d'information sur des réseaux comme **TOR**. Une démarche qui rappelle le projet **Memex** mené par la **Darpa**. L'agence pour les projets de recherche avancés de défense américaine a, en effet, récemment créé un « *Google du Deep Web* » afin d'aider la police dans ses enquêtes en tout genre.

Le C3N s'emploie également à scruter les jeux en ligne. « *Les auteurs détournent de plus en plus les jeux en ligne comme **Clash of Clan**, **Call of Duty** ou encore **Oh My Dollz*** », assure le spécialiste. « *Sur Clash of Clan, par exemple, nous avons identifié en 2015 plusieurs dizaines de cas d'apologie du terrorisme et de menaces d'attentats* ».

Outre les logiciels, le C3N mise également sur les compétences humaines. L'unité a récemment recruté plusieurs officiers commissaires, dont un docteur en informatique, un ingénieur en électronique et un universitaire spécialiste des systèmes d'information.



Réagissez à cet article

**Source : Cybercriminalité : la boîte à outils des gendarmes du Net**