La cybercriminalité a de belles années devant elle

	La cybercriminalité a de belles années devant elle

Les prochaines années laissent entrevoir de beaux moments pour les cybercriminels de tout acabit. Les raisons expliquant cela sont nombreuses. Quelles sont-elles?

Suivre la scène de la sécurité informatique a ceci de particulier : c'est à la fois fascinant et grandement décourageant. C'est d'autant plus décourageant que les tendances présentes au cours des derniers mois laissent entrevoir de beaux jours pour les cybercriminels. Essentiellement, quatre raisons expliquent cela.

La multiplication des cibles potentielles

La première raison est assez évidente : il y a de plus en plus de cibles disponibles pour les criminels. La surmultiplication du nombre de plateformes exploitant Internet a pour effet de toutes les transformer en des opportunités potentielles pour des gens malintentionnés. La manifestation la plus flagrante de cette surmultiplication se transpose dans la fulgurante montée de l'Internet des objets.
Ce nouvel eldorado porte toutefois les gènes de sa propre insécurité. En effet, le marché est meublé par une multitude de joueurs, et leur intérêt porté à la chose sécuritaire est tout aussi variable. Ainsi, alors que l'objectif est d'occuper le marché le plus rapidement possible, bon nombre de joueurs impliqués dans la course à l'Internet des objets arrivent sur le marché avec des produits qui sont, volontairement ou involontairement, plus ou moins sécurisés.
Bref, nous sommes placés devant un cercle vicieux duquel nous ne pouvons pas nous sortir : plus de technologies signifient nécessairement plus de vulnérabilités et, conséquemment, plus d'opportunités criminelles. De plus, croire que l'on puisse mettre un frein à l'évolution technologique est illusoire.

Le difficile marché de la sécurité

Le contexte actuel rend les ressources extrêmement difficiles à conserver ou à acquérir pour les petites et moyennes entreprises qui n'ont pas les moyens d'offrir des salaires élevés.
Alors que le domaine apparaît comme extrêmement complexe, le manque criant de main-d'œuvre est de plus en plus problématique dans les entreprises. Forbes affirme pourtant que ce secteur vaudra sous peu 75 milliards de dollars US et que le marché créera plus d'un million d'emplois.
Non seulement manque-t-il de spécialistes en sécurité, mais il manque aussi de plus en plus de pirates black hat sur le marché, faisant en sorte que les cybercriminels eux-mêmes se tournent de plus en plus vers des modèles de sous-traitance pour effectuer leurs opérations.
Ce manque d'expertise a pour effet de rendre l'économie globalement plus ou moins axée sur la sécurité. Certes, certains secteurs ont les moyens de leurs ambitions, mais le contexte actuel rend ces ressources extrêmement difficiles à conserver ou à acquérir pour les petites et moyennes entreprises qui n'ont pas les moyens d'offrir des salaires élevés. Les effets sont bien sûr conséquents : la situation engendre une sécurité bien inégale, avec le lot de vulnérabilités qu'elle impose.

La rentabilité évidente

Autre point extrêmement important pour expliquer pourquoi la cybercriminalité aura le vent dans les voiles? C'est lucratif. La logique criminelle est relativement simple : il s'agit de faire le plus d'argent possible, le plus facilement possible. En somme, c'est le capitalisme en action.
Dans le domaine de la cybercriminalité, cela fonctionne décidément. On estime à 445 milliards de dollars US le marché de la cybercriminalité. Bon, je vous entends déjà geindre et dire que c'est fort de café. Soit. Admettons que ce soit la moitié moins, c'est tout de même 222 milliards, batinse!
Pour rappel, le budget du Canada est d'environ 290 milliards de dollars CA. C'est donc payant, et c'est bien dommage, mais les conséquences de la cybercriminalité sont minimes. Les chances d'arrêter les criminels sont plutôt basses (voir point suivant) et les peines encourues ne sont pas adaptées.

L'incapacité d'action des agences d'application de la loi

Les cybercriminels ont donc le beau jeu, puisque le risque de se faire prendre est extrêmement bas. En effet, les forces policières sont mal équipées pour confronter la cybercriminalité, faisant en sorte que trop souvent, elles doivent capituler devant les actions commises par les criminels. Dans les cas les plus extrêmes, les agences tenteront de déployer les efforts nécessaires pour faire culminer une enquête, mais cela se fera à grands coups de contrats avec le secteur privé afin de se procurer l'expertise nécessaire pour résoudre le crime en question. Le fait que le FBI ait versé un montant de 1,3 million à un groupe de «chercheurs en sécurité», considérés par plusieurs comme ayant des mœurs on ne peut plus douteuses, pour accéder aux données présentes dans l'iPhone du terroriste de San Bernardino en est, en soi, la manifestation la plus éloquente.
Lutter contre la cybercriminalité demande essentiellement quatre choses. Une culture particulière, une collaboration internationale, des moyens et des techniques disponibles, et des compétences de pointe dans le domaine des technologies. Le dur constat qu'il faut faire, c'est qu'outre la collaboration internationale, les autorités compétentes n'ont pas les moyens pour atteindre les trois autres prérequis. Par conséquent, la vaste majorité des corps policiers ne s'attaqueront aux cybercrimes que lorsque les infractions sont trop exagérées.

La somme de toutes les peurs

Au final, ce qui est le plus inquiétant dans cette situation, c'est que plus le temps avance, plus les réseaux de cybercriminels deviennent solides, sophistiqués et ont de plus en plus de moyens. Les laisser agir en toute impunité a pour effet de les rendre toujours plus coriaces, ce qui rendra la tâche de lutter contre eux d'autant plus difficile à long terme. Il faudra que l'on prenne le problème à bras le corps une fois pour toute, sinon, nous risquons d'avoir de mauvaises surprises dans les prochaines années.
Article original de branchez-vous.com

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 : La cybercriminalité a de belles années devant elle | Branchez-vous

---

Alerte : un malware Android commandé par… Twitter

Alerte : un malware Android commandé par… Twitter

Les concepteurs du malware Android Twittor se servent du réseau social pour envoyer des instructions à la souche infectieuse. Une technique plus furtive que les classiques serveurs de commande et contrôle.

L'éditeur d'antivirus Eset affirme avoir découvert le premier malware commandé… par des tweets. Selon la société slovaque, Android/Twittor est une application Android malveillante, probablement diffusée par SMS ou via des URL piégées, qui masque sa présence et se connecte à un compte Twitter dans l'attente d'instructions. Ces dernières peuvent le conduire à télécharger une autre app malveillante ou à changer de compte Twitter de contrôle. Actuellement, selon Eset, Twittor sert à importer différentes versions d'un malware bancaire. Mais pourrait tout aussi bien passer au ransomware…

« *Utiliser Twitter plutôt que des serveurs de commande et contrôle (C&C) est plutôt innovant pour un botnet Android* », souligne Lukas Stefanko, le chercheur d'Eset qui a mis au jour cette nouvelle souche infectieuse. L'objectif des cybercriminels est, comme l'indique ce chercheur, de constituer un réseau de machines esclaves, soit un botnet. Le point faible des constructions de ce type réside souvent dans l'envoi régulier d'instructions aux éléments de ce réseau, des communications susceptibles de révéler l'existence du botnet. Par ailleurs, les serveurs C&C constituent le maillon faible des botnets : si les autorités les localisent et parviennent à les fermer, c'est tout le réseau criminel qui s'effondre.

Passer d'un compte Twitter à un autre

Autant de raisons qui pourraient avoir poussé les concepteurs de Twittor à complexifier les techniques de communication entre les machines esclaves et l'entité les contrôlant, selon Eset. En plus de l'emploi de Twitter, les cybercriminels chiffrent leurs messages et utilisent des topologies complexes pour leur architecture de C&C, avance l'éditeur. « *Ces canaux de communication sont difficiles à mettre au jour et encore plus difficiles à bloquer totalement*, reprend Lukas Stefanko. *De l'autre côté, il est très simple pour les escrocs de rediriger les communications vers un compte nouvellement créé.* » Et pas de risque de voir la police fermer purement et simplement Twitter pour ce motif…

Dans l'univers Windows, dès 2009, un botnet a eu recours à Twitter, fondé seulement 3 ans auparavant, pour envoyer des instructions. Mais Twittor est bien le premier malware créateur de bot commandé via le réseau social.

Article original de Reynald Fléchaux

Réagissez à cet article

Original de l’article mis en page : Inédit : un malware Android commandé par… Twitter

---

Pourquoi le Conseil d’État autorise une exploitation de données saisies via l’état d’urgence ?

Pourquoi le Conseil d’État autorise une exploitation de données saisies via l’état d’urgence ?

Alors que le tribunal en première instance avait jugé que les éléments n'étaient pas réunis pour justifier une telle procédure extra-judiciaire, le Conseil d'État a autorisé la police à exploiter des données informatiques saisies à Roubaix chez un suspect ayant fait l'objet d'une perquisition administrative.

À la suite de l'attentat de Nice, le gouvernement a réintégré en juillet dernier dans le dispositif de l'état d'urgence la possibilité pour la police de procéder à la saisie de matériels ou données informatiques présentes ou accessibles sur les lieux d'une perquisition administrative. Mais conformément aux préconisations du Conseil constitutionnel, il l'a fait en assortissant cette entorse à la vie privée et au droit de propriété d'un certain nombre de garanties minimales.
En particulier, il est désormais précisé que de tels matériels et données ne peuvent être saisis que « *si la perquisition révèle l'existence d'éléments, notamment informatiques, relatifs à la menace* » que représenterait la personne visée. Par ailleurs, les policiers ne peuvent rien faire des données saisies sans l'autorisation d'un juge des référés d'un tribunal administratif, qui a 48 heures pour donner son aval.

Or Nextinpact rapporte que le ministère de l'intérieur a dû faire appel d'une décision défavorable du tribunal administratif de Roubaix, pour avoir le droit d'exploiter les données saisies chez un suspect. Sur place, la perquisition et la fouille des données informatiques accessibles n'avait apporté strictement aucun élément matériel permettant d'étayer une éventuelle infraction pénale du justiciable. Le juge de première instance en avait donc déduit qu'il ne pouvait pas autoriser l'exploitation des données injustement saisies.
Ce faisant, le juge restait dans l'esprit de l'avis du Conseil constitutionnel, qui s'opposait aux saisies et exploitations de données « *alors même qu'aucune infraction n'est constatée* ».
L'INTÉRESSÉ A INDIQUÉ COMMUNIQUER AVEC EUX AU MOYEN DE SON TÉLÉPHONE PORTABLE, EN USANT NOTAMMENT DE MESSAGERIES INSTANTANÉES OU CRYPTÉES

Mais le Conseil d'État, lui, en reste à une lecture plus littérale de ce que le gouvernement a écrit dans la nouvelle loi, qui n'a pas été soumise au Conseil constitutionnel. Celle-ci ne demande pas qu'une infraction soit constatée, mais uniquement que la perquisition « révèle l'existence d'éléments », matériels ou non, relatifs à la menace. C'est beaucoup plus vague.

Or la haute juridiction administrative note dans son ordonnance (.pdf) que « l'intéressé a déclaré au cours de la perquisition être resté en contact avec quatre amis de Roubaix, qu'il a nommément désignés, partis en Syrie et en Irak pour y mener le djihad », et qu'il « a indiqué communiquer avec eux au moyen de son téléphone portable, en usant notamment de messageries instantanées ou cryptées ». Ces déclarations sont donc en elles-mêmes des éléments relatifs à la menace que pourrait représenter l'individu, qui justifient d'autoriser l'exploitation des données saisies.

UNE OBLIGATION DE RESTITUTION SOUS 15 JOURS

Cette affaire fera certainement redire aux avocats qu'il est toujours primordial de garder le silence, mais il faut noter que le suspect semble pleinement coopératif, et qu'il a accepté que ses données soient inspectées. Il a peut-être préféré que son innocence soit ainsi vérifiée, plutôt que sa présomption d'innocence reste, dans l'esprit des services de renseignement, une présomption de culpabilité.
Selon le PV de perquisition, la police avait procédé à la saisie d' « un ordinateur de marque ACER et de son chargeur, d'un téléphone portable de marque Apple et de son chargeur, d'une clef USB rouge de marque Emtec d'une capacité de 16 Gb, d'une clé USB noire de marque Verbatim d'une capacité de 16 Gb, d'une carte SD de marque Viking d'une capacité de 512 Mb et d'une carte SD de marque Sandisk d'une capacité de 8 Gb ».
Selon les termes de la loi, l'ensemble de ces matériels doivent être retournés à leur propriétaire dans les 15 jours suivant l'autorisation (délivrée ici par ordonnance du 23 août), sans prorogation motivée ou découverte d'éléments probants. Les données non pertinentes devront être détruites sous un délai de 3 mois.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Pourquoi le Conseil d’État autorise une exploitation de données saisies via l’état d’urgence – Politique – Numerama

---

Comment se prémunir de la cybercriminalité, ce risque sur Internet pour les particuliers et les professionnels ?

Comment se prémunir de la cybercriminalité, ce risque sur Internet pour les particuliers et les professionnels ?

En pleine recrudescence, de nombreuses attaques ciblent les particuliers mais aussi les entreprises et les administrations. Elles visent à obtenir des informations personnelles afin de les exploiter ou de les revendre (données bancaires, identifiants de connexion à des sites marchands, etc.). Hameçonnage (phishing) et «Rançongiciel» (ransomware) sont des exemples connus d'actes malveillants portant préjudices aux internautes.
Pour s'en prémunir, des réflexes simples existent.

QUELS SONT LES DIFFERENTS TYPES D'ATTAQUES ?

Attaque par hameçonnage (phishing)

L'hameçonnage, phishing ou filoutage est une technique malveillante très courante sur Internet. L'objectif : opérer une usurpation d'identité afin d'obtenir des renseignements personnels et des identifiants bancaires pour en faire un usage criminel.

1. Le cybercriminel se « déguise » en un tiers de confiance (banques, administrations, fournisseurs d'accès à Internet…) et diffuse un mail frauduleux, ou contenant une pièce jointe piégée, à une large liste de contacts. Le mail invite les destinataires à mettre à jour leurs informations personnelles (et souvent bancaires) sur un site internet falsifié vers lequel ils sont redirigés.
2. La liste comprend un nombre si important de contacts et augmente les chances que l'un des destinataires se sente concerné par le message diffusé.
3. En un clic, il est redirigé vers le site falsifié qui va recueillir l'ensemble des informations qu'il renseigne.
4. Ces informations sont alors mises à disposition du cybercriminel qui n'a plus qu'à faire usage des identifiants, mots de passe ou données bancaires récupérées.

Voir la vidéo de la Mackacademy sur le phishing (CIGREF – partenariat ANSSI)

Pour s'en prémunir :

- N'ayez pas une confiance aveugle dans le nom de l'expéditeur de l'email. Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre biais.
- Méfiez-vous des pièces jointes, elles pourraient être contaminées. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.
- Ne répondez jamais à une demande d'informations confidentielles par mail.
- Passez votre souris au-dessus des liens, faites attention aux caractères accentués dans le texte ainsi qu'à la qualité du français ou de la langue pratiquée par votre interlocuteur (ex : orthographe).

Pour aller plus loin, n'hésitez pas à consulter la page sur les conseils aux usagers qui reprend les bonnes pratiques à mettre en place pour sécuriser ses équipements et ses données.

Attaque par «Rançongiciel» (ransomware)

Les rançongiciels sont des programmes informatiques malveillants de plus en plus répandus (ex : Locky, TeslaCrypt, Cryptolocker, etc.). L'objectif : chiffrer des données puis demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

1. Le cybercriminel diffuse un mail qui contient des pièces jointes et / ou des liens piégés. Le corps du message contient un message correctement rédigé, parfois en français, qui demande de payer rapidement une facture par exemple.
2. En un clic, le logiciel est téléchargé sur l'ordinateur et commence à chiffrer les données personnelles : les documents bureautiques (.doc, .xls, .odf,etc), les photos, la musique, les vidéos…etc.
3. Les fichiers devenus inaccessibles, un message s'affiche pour réclamer le versement d'une rançon, payable en bitcoin ou via une carte prépayée, en échange de la clé de déchiffrement. Attention, rien n'indique que le déchiffreur en question soit efficace !

Pour s'en prémunir :

- N'ayez pas une confiance aveugle dans le nom de l'expéditeur de l'email. Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre biais.
- Méfiez-vous des pièces jointes et des liens dans les messages dont la provenance est douteuse. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.
- Effectuez des sauvegardes régulièrement sur des périphériques externes.
- Mettez à jour régulièrement tous vos principaux logiciels en privilégiant leur mise à jour automatique.

Pour aller plus loin, n'hésitez pas à consulter la page sur les conseils aux usagers qui reprend les bonnes pratiques à mettre en place pour sécuriser ses équipements et ses données.

VOUS ÊTES VICTIME D'UN RANSOMWARE OU DE FISHING ?

Suite à une escroquerie ou une cyberattaque, déposez plainte auprès d'un service de **Police nationale** ou de **Gendarmerie nationale** ou bien adressez un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent.

Munissez-vous de tous les renseignements suivants :

- Références du (ou des) transfert(s) d'argent effectué(s)
- Références de la (ou des) personne(s) contactée(s): adresse de messagerie ou adresse postale, pseudos utilisés, numéros de téléphone, fax, copie des courriels ou courriers échangés…
- Numéro complet de votre carte bancaire ayant servi au paiement, référence de votre banque et de votre compte, et copie du relevé de compte bancaire où apparaît le débit frauduleux
- Tout autre renseignement pouvant aider à l'identification de l'escroc

Vous pouvez également signaler les faits dont vous avez été victime via la plateforme de signalement « Pharos » ou le numéro dédié : 0811 02 02 17

Des services spécialisés se chargent ensuite de l'enquête :

- **Police nationale** : l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) qui dépend de la Sous-direction de lutte contre la cybercriminalité (SDLC) : 01 47 44 97 55
- **Gendarmerie nationale** : le centre de lutte contre les criminalités numériques (C3N) du Service Central du Renseignement Criminel (SCRC) :cyber@gendarmerie.interieur.gouv.fr
- **Préfecture de police** : la Préfecture de police de Paris, de la Direction centrale du renseignement intérieur (DCRI) et ses équipes de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) compétente uniquement pour Paris et petite couronne (75, 92, 93 et 94) : 01 40 79 67 50

Article original de gouvernement.fr

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

- Expertises techniques (virus, spyware, 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

Contactez nous

Réagissez à cet article

Original de l'article mis en page : Cybercriminalité | Gouvernement.fr

---

Comment être payé pour lancer des attaques informatiques de type DDoS

Comment être payé pour lancer des attaques informatiques de type DDoS

Déjà que lancer des DDoS était accessible au premier idiot du village, voilà que maintenant, il pourrait être possible de les payer pour leurs attaques.

Le DDoS, une plaie du web qui a pour mission de bloquer un serveur à coups de connexions de masse. Un Déni Distribué de Service, c'est un peu comme déverser des poubelles devant l'entrée d'une maison, plus personne ne peut rentrer, plus personne ne peut en sortir. Deux chercheurs américains viennent de rajouter une couche dans ce petit monde fou-fou des DDoSeurs : payer les lanceurs d'attaques.

Eric Wustrow de l'Université du Colorado et Benjamin VanderSloot de l'Université du Michigan se sont lancés dans la création d'une crypto-monnaie, comme le bitcoin, qui pourrait rémunérer les lanceurs de DDoS. Ils ont baptisé leur « idée » : DDoSCoin. Sa mission, récompenser les participants à des dénis de service distribués (DDoS). Cette « monnaie » ne fonctionne que lorsque l'ordinateur de la cible a le TLS activé (Security Layer Transport), un protocole de chiffrement pour les communications Internet sécurisée.

Créer une monnaie qui permet aux « mineurs » de prouver leur participation à un DDoS vers un serveur web ciblé peut paraitre bizarre. Les deux étudiants cherchent des méthodes pour contrer et remonter ce type d'attaque.

Article original de Damien Bancal

Vous comprendrez que le titre de cet article n'a pas pour but de vous inciter à utiliser cette technique, mais plutôt de vous faire découvrir qu'elle existe pour l'anticiper.

Denis Jacopini

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

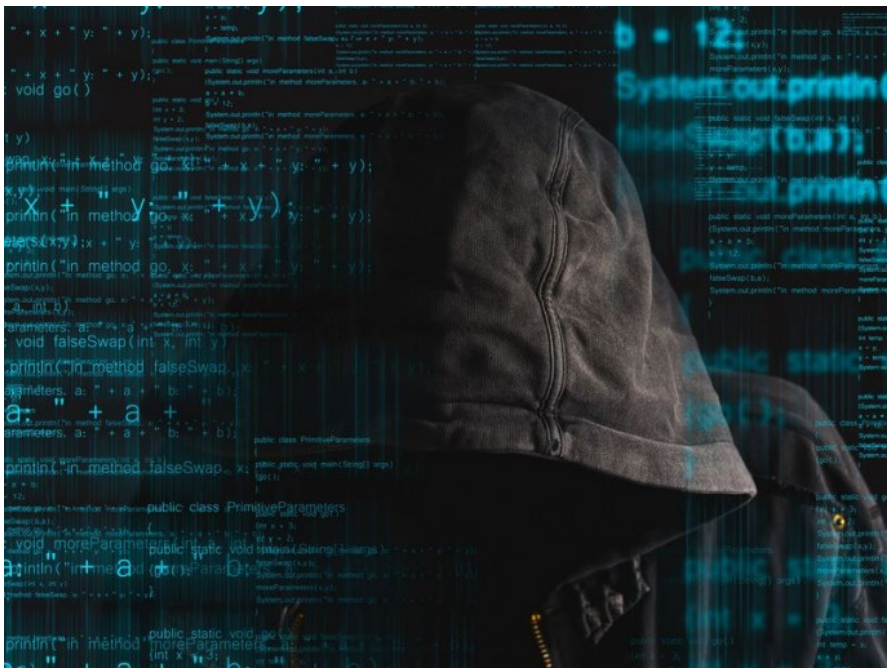
Réagissez à cet article

Original de l'article mis en page : Être payé pour lancer des DDoS – Data Security BreachData Security Breach

---

Shadow Brokers, une affaire

de Cyberespionnage



Shadow Brokers, une affaire de Cyberespionnage

Tour d'horizon des conséquences d'une affaire de cyber-espionnage au retentissement international alors que les fichiers mis en ligne par les mystérieux Shadow Brokers, et probablement dérobés à la NSA, commencent à livrer leurs secrets.

1) Pourquoi un tel intérêt pour les Shadow Brokers ?

Lundi 15 août, un groupe de hackers appelé Shadow Brokers a annoncé avoir piraté des systèmes informatiques utilisés par Equation, une organisation réputée proche de la NSA. A l'appui de ses affirmations, ce groupe jusqu'alors inconnu a posté deux archives sur des sites de partage. La première, en libre accès, renferme 300 Mo de données, où se mêlent des outils et des techniques pour infiltrer des systèmes…. [lire la suite]

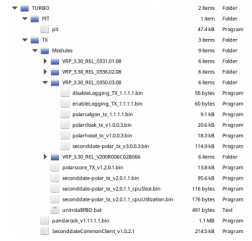
2) Le hacking de la NSA est-il établi ?

Bien entendu, ni la célèbre agence américaine ni le groupe de hackers Equation, réputé proche de celle-ci, n'a confirmé que les outils mis en ligne par les Shadow Brokers provenaient bien de leurs serveurs. Mais plusieurs éléments concordants établissent un lien direct entre les fichiers mis en ligne par les Shadow Brokers et le couple NSA/Equation. D'abord, c'est l'éditeur russe Kaspersky qui remarque que plus de 300 fichiers présents dans la première archive utilisent une implémentation des algorithmes de chiffrement RC5 et RC6 identique à celle utilisée par le groupe Equation. « *La probabilité que tout ceci (l'archive mise en ligne, NDLR) soit un faux ou ait été conçu par rétro-ingénierie est extrêmement faible* », écrivent les chercheurs de Kaspersky dans un billet de blog. [lire la suite]

3) Que dit cette affaire du groupe Equation ?

Le nom de ce groupe, choisi en raison de sa prédilection pour les techniques de chiffrement de haut vol, a été donné début 2015 par Kaspersky à un groupe de hackers, que l'éditeur russe décrivait alors comme le plus techniquement doué qu'il ait jamais identifié. La société parlait alors « *d'une menace qui dépasse tout ce qui est connu en termes de complexité et de sophistication des techniques employées, une menace active depuis au moins deux décennies* ». Equation exploitait depuis 2008 des failles zero day qui ne seront mises à jour que plus tard, à l'occasion du piratage du nucléaire iranien par Stuxnet. [lire la suite]

4) Que renferme l'archive des Shadow Brokers ?



Plusieurs chercheurs en sécurité se sont déjà penchés sur le cyber-arsenal mis à disposition par les Shadow Brokers (lire notamment l'analyse de Mustafa Al-Bassam ou la synthèse réalisée par *Softpedia*). On y trouve des *exploits*, autrement dit des codes d'exploitation permettant de prendre le contrôle ou d'espionner des pare-feu ou passerelles VPN fournis par de grands constructeurs comme Cisco, Juniper ou Fortinet. Des constructeurs qui ont déjà reconnu que les outils mis en ligne menaçaient bien certains de leurs matériels. Mais, dans tous les cas, il s'agit de générations anciennes de machines. Les appliances Cisco Pix, ciblées par plusieurs outils, ne sont par exemple plus supportées par le constructeur depuis 2009. [lire la suite]

5) L'archive a-t-elle livrée tous ses secrets ?

Et il y a aussi les outils dont la vocation ne se limite pas à cibler une gamme de machines en particulier. *The Intercept* explique ainsi que des éléments d'une architecture exploitée par la NSA pour mettre en place des attaques de type Man-in-the-Middle, autorisant l'interception de requêtes Web, figurent dans l'archive des Shadow Brokers.Sans risque de se tromper, la réponse est non. « *Comme il y a 300 Mo de code, de documentations, de binaires, personne n'a publié d'analyse complète* », remarquent Hervé Schauer et Christophe Renard.[lire la suite]

6) Quels sont les risques pour les entreprises ?

Voir de tels outils mis à la disposition de cybercriminels est évidemment inquiétant. « *On est ici face à des outils d'attaque de haut niveau, mis librement à disposition sur le Web*, explique Gérôme Billois. *Les entreprises doivent donc être très attentives, effectuer l'inventaire des matériels exposés sur leur parc et apporter les modifications nécessaires pour protéger leurs infrastructures. Heureusement, les exploits mis au jour sont assez anciens et ciblent donc du matériel âgé. Mais certaines machines peuvent toujours être en exploitation.* » Au fur et à mesure que les codes de l'archive des Shadow Brokers seront décortiqués, des correctifs et des indicateurs de compromission vont être publiés. Ce qui permettra aux RSSI de contrer la menace. C'est donc plutôt une course de fond qui s'engage. [lire la suite]

7) Qui a fait le coup ?

La liste des suspects s'est très vite limitée à quelques noms. Très rapidement, Nicolas Weaver, de l'université de Berkeley, pointe la Chine, soupçonnée de nombreux actes de cyber-espionnage contre les intérêts américains, et la Russie. Une seconde hypothèse que défend lui aussi Edward Snowden, précisément réfugié en Russie après avoir été à l'origine de la plus importante fuite de données de l'histoire de la NSA. [lire la suite]

8) Un second lanceur d'alertes à la NSA ?

Car une autre hypothèse a également de nombreux partisans : celle de l'implication d'un 'insider', un nouveau lanceur d'alerte à la NSA. Plusieurs éléments viennent étayer cette hypothèse. Primo, l'archive en question renferme différentes versions d'un même outil, des manuels d'utilisation ou des fichiers à vocation interne. Ce qui cadre mal avec l'hypothèse d'un serveur d'attaque, ou d'un serveur de pré-production, qui aurait été compromis par un assaillant externe. [lire la suite]

9) Quelles sont les conséquences possibles ?

D'ores et déjà, la fuite a dû déclencher un branle-bas de combat au sein de la NSA, qui doit chercher l'origine de cette encombrante archive et, surtout, comment mettre fin aux révélations successives sur ses activités offensives. L'agence devra également s'assurer qu'elle n'exploite plus les codes révélés au public pour ses opérations actuelles. Car, très rapidement, les outils de sécurité seront en mesure de détecter les signatures des outils révélés par les Shadow Brokers.[lire la suite]

10) Qu'en pense Bernard Cazeneuve ?

Passée la boutade, le ministre de l'Intérieur français, qui entend prendre la tête d'une initiative internationale permettant d'encadrer le chiffrement, a devant les yeux une autre illustration des limites que pointent de nombreux spécialistes, y compris le Conseil national du numérique (CNNum).Après l'affaire Juniper (le constructeur avait employé un algorithme de chiffrement affaibli par la NSA, qui avait été détourné par un acteur inconnu), les révélations des Shadow Brokers illustrent une fois encore le caractère spécifique des armes cyber.[lire la suite]

Article original de Reynald Fléchaux

Réagissez à cet article

Original de l’article mis en page : Cyberespionnage : 10 questions pour comprendre l’affaire Shadow Brokers

---

Votre vie privée numérique en danger sur Leakedsource

Votre vie privée numérique en danger sur Leakedsource

Depuis quelques semaines, le site leakedsource engrange des centaines de millions de données volées par des pirates informatiques. Un business juteux qui met en danger des millions d'internautes.

LeakedSource, nouvelle source d'informations pour pirates informatiques ? Souvenez-vous, on vous parlait en juillet, de données volées appartenant à un ancien garde du corps de Vladimir Poutine, le Président Russe, ou encore de Nicolas Sarkozy, ancien Président de la République Française. Son identité, ses données privées, des courriels… Un piratage qui semblait être particulièrement compliqué à orchestrer tant les sources d'informations concernant ce body guard étaient variés. Après enquête, j'ai découvert que si le résultat pouvait être particulièrement préjudiciable pour la cible, la mise en place et l'exécution de cette attaque était aussi simple que « *1 + 1 font 2*« .

Leakedsource, source quasi inépuisable de malveillances

Pour ce garde du corps, mais aussi pour de nombreuses personnalités, le risque est énorme. Tout débute par le piratage de centaines de bases de données de part le monde. Myspace, Adobe, Linkedin, Twitch , Xat , Badoo… ne sont que des exemples parmi d'autres. Je gère, avec le protocole d'alerte ZATAZ, des dizaines de fuites de données par mois concernant des PME et entreprises Françaises. Imaginez donc ce que brassent des sites comme leaked source.

Leakedsource.com, un espace web tenu par des Russes, a pour mission de regrouper les informations volées par des pirates et de permettre de consulter les informations en question. Les administrateurs du portail expliquent que leur service est fait pour s'assurer que les données volées ne vous concernent pas. Sauf que, des données, il y en a des centaines de millions, et vous pourriez bien vous y retrouver, comme Mark Zuckerberg, cofondateur et directeur général de Facebook, piraté en juin 2016 parce que son mot de passe « *DaDaDa* » était accessible dans une base de données piratées et stockées chez Leakedsource.

Vous ne risquez rien ? Vraiment ?

Cela n'arrive qu'aux autres ? Allez donc regarder du côté de vos données. C'est d'ailleurs ce qu'aurait dû faire l'auteur des jeux vidéo Garrysmod et de Rust, Garry Newman. J'ai pu avoir une longue conversation avec l'auteur de divertissements vidéo ludique qui ne s'attendaient pas à découvrir sa vie numérique mise en pâture de la sorte. Il faut dire aussi que plusieurs pirates ont contacté la rédaction de ZATAZ.COM pour se vanter d'avoir mis la main sur ses données Paypal, Amazon, gMail de ce créateur de jeux vidéo britannique. Bref, pour 4 dollars (le prix journalier d'un abonnement Leaked source pour accéder aux données) n'importe quel internaute peut se transformer en vulgaire violeur de vie 2.0. Il suffit de rentrer un mail, un pseudonyme ou encore une adresse IP et Leakedsource cherche dans ses bases de données la moindre concordance. Cerise sur le gâteau, quand le mot de passe est hashé, donc illisible à la première lecture, Leaked source propose la version du précieux sésame déchiffré. « ***Si les personnes [les pirates, NDR) sont malines, elles peuvent faire beaucoup de dégâts avec ce genre d'outil accessible à Monsieur tout le monde*** » me confirme un utilisateur.

Que faire pour éviter ce type de fuite de données ?

Je vais très rapidement être honnête avec vous, si vous mettez vos données en ligne, dites vous qu'elles ne sont plus en sécurité. Et ce n'est pas notre vénérable CNIL qui pourra vous aider. Avec plusieurs centaines de cas de fuite de données que je traite avec le protocole d'alerte de zataz par an, j'ai déjà pu croiser mes propres informations. Je vous parlais plus haut de Leakedsource, j'ai pu y retrouver mon compte Adobe. Pourtant, le géant du logiciel l'avait juré, il était « *secure* » [sécurisé, ndr].

Tellement « *secure* » qu'un de mes mails, et le mot de passe attenant, sont disponible dans ce big data du malveillant. Autant dire que l'adresse mail et le mot de passe en question ont été détruits et ne seront plus utilisés.

Que faire donc ? D'abord, un compte mail par service. Je sais, c'est long est fastidieux. Mais je pense qu'il va être beaucoup plus long et fastidieux pour Garry Newman de revalider l'ensemble de ses comptes « infiltrés », car il utilisait la même adresse électronique pour ses accès Paypal, Amazon…

Ensuite, ne mettez pas le même mot de passe pour l'ensemble de vos services en ligne. On a beau le répéter, cesser de vous croire plus malin que les 010101 qui nous régissent. Mark Zuckerberg et son « *DaDaDa* » lui ont coûté son Twitter et son Pinterest. Pour Garry, plus grave encore, son compte Amazon et Paypal, avec des données sensibles [adresses postales, données bancaires…] qui ne devraient pas être disponibles à la planètes web. Donc, oui, c'est fastidieux, mais un mot de passe par compte est une obligation.

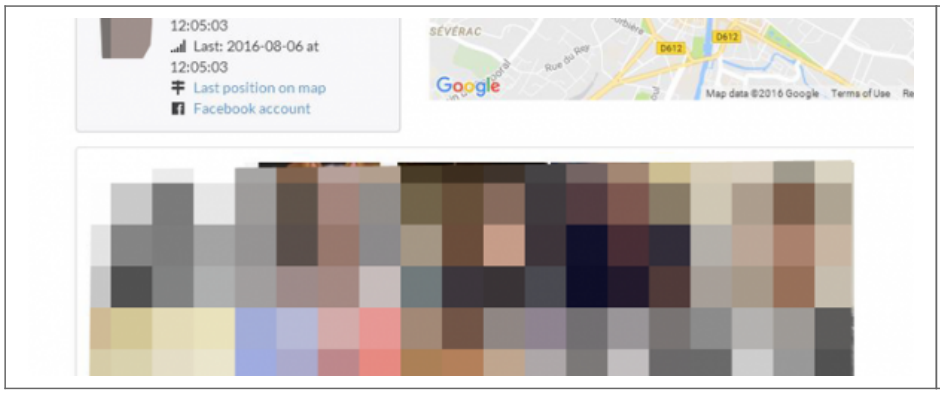
Pour finir, en ce qui concerne l'IP, n'hésitez plus à utiliser un VPN. L'outil permet de cacher votre véritable adresse de connexion, en plus de chiffrer vos informations transitant sur la toile. Je vous invite à regarder du côté de nos partenaires et amis de chez **NoLimitVPN** ou encore HMA! pour blinder vos connexions PC, Mac et mobiles.

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Leakedsource, le site qui met en danger votre vie privée – ZATAZ

Géolocaliser un téléphone mobile en deux clics de souris



Géolocaliser un téléphone mobile en deux clics de souris

Cyber géolocaliser un porteur de téléphone est de plus en plus simple. Un chercheur en informatique montre à ZATAZ.COM comment créer un tracker maison devient simple comme bonjour.

Les téléphones portables, de nos jours, sont de véritables ordinateurs aux capacités de traçage, surveillance et cyber surveillance qui fait froid dans le dos. Regardez, prenons les exemples tels que Facebook et son option « amis à proximité » ou encore PokemonGo et sa capacité de géolocalisation. Du traçage au centimètre. Des technologies de « ciblage » qui deviennent simple à créer et à utiliser. Tristan, informaticien Parisien, vient de contacter ZATAZ pour présenter son cas d'étude : un outil de traçage en temps réel capable de tracer l'itinéraire de ses cibles.

Géolocaliser un téléphone : Souriez, vous êtes pistés

Depuis quelques temps Tristan s'intéresse aux applications proposées dans les mobiles, et plus précisément aux logiciels qui font transiter des informations telles que des positions de latitude et de longitude. Avec un associé, il a lancé Lynx Framework, une entité spécialisée dans la création d'outils de sécurité pour les applications web.
A parti de ses recherches, Tristan a créé un outil de « traque », de quoi géolocaliser un téléphone qui met à jour les dangers de nos mobiles et de leurs capacités à indiquer notre emplacement, mais aussi, nos itinéraires. « ***En analysant les requêtes envoyées par certaines applications je me suis rendu compte qu'il serait possible de récupérer le positionnement de plusieurs personnes en même temps et de les positionner sur une carte de type google map.*** » m'explique le chercheur.

A l'image des sauvegardes de Google Map que je vous indiquais en 2015, l'outil « privé » de Tristan fait pareil, mais en plus discret encore. Via un outil légal et disponible sur Internet, Burp Suite, notre chercheur a analysé les requêtes envoyées par plusieurs logiciels de rencontres disponible dans le Google Play.

Comment cela fonctionne-t-il ?

« *Le tracker prend le contrôle de plusieurs comptes d'application de rencontre et récupère la position des personnes à proximité,* indique-t-il à ZATAZ.COM. *Il ajoute ces informations dans sa base de données et vérifie l'existence des positions pour cette identité. » Si l'application de Tristan retrouve la même personne, mais pas à la même position, il va créer un itinéraire de l'individu via son ancienne position*« . Nous voilà avec la position et le déplacement exacts d'un téléphone, et donc de son propriétaire, à une heure et date données.

Géolocaliser un téléphone : Chérie, tu faisais quoi le 21 juillet, à 12h39, à 1 cm de ta secrétaire ?

Après quelques jours de recherche, Tristan a mis en place une base de données de déplacement dans une ville. Une commune choisie au hasard. Son outil est en place, plusieurs systèmes sont lancés : Une carte avec le positionnement des personnes croisées ; une page plus explicite pour chaque personne avec la date de croisement, son âge… ; une page ou notre chercheur gère ses comptes dans l'application. Bonus de son idée, un système d'itinéraire complet a été créé. Il permet de tracer un « chemin » de déplacement si la personne croisée a déjà été croisée dans le passé, dans un autre lieu. « J'ai positionné un compte au centre de la ville, un autre à l'entrée et le suivant à la sortie, ce qui a données en quelques heures une 50ène de données » confie-t-il « Il est inquiétant de voir autant de données personnelles transitées en clair via ces applications ».

Géolocaliser un téléphone : détournement possible d'un tel « tracker » ?

Vous l'aurez compris, « tracer » son prochain est facilité par ses applications qui ne protègent pas les informations de positionnement des utilisateurs. Il devient possible d'imaginer une plateforme, en local, avec plusieurs comptes positionnés à des endroits différents dans une ville. Bilan, suivre plusieurs individus devient un jeu d'enfant. Si on ajoute à cela les applications de déplacement de type UB, qui communique les données de ses chauffeurs par exemple, ainsi que celles d'autres réseaux sociaux, il devient réellement inquiétant de se dire que positionner une personne et la tracer se fait en quelques secondes. Deux solutions face à ce genre de traçage : jeter votre portable ou, le mieux je pense, forcer les éditeurs d'applications à vérifier la sécurisation des données envoyées, et les chiffrer pour éviter qu'elles finissent en clair et utilisable par tout le monde.
Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Géolocaliser un téléphone mobile en deux clics de souris – ZATAZ

Découvrez la faille qui ouvre toutes les Volkswagen sans clef

Découvrez la faille qui ouvre toutes les Volkswagen sans clef

---

Tous les véhicules vendus par Volkswagen depuis environ 20 ans peuvent être ouverts sans clef. Et la technique mise au point par des chercheurs de l'université de Birmingham fonctionne aussi avec d'autres constructeurs.

Nul doute que Volkswagen aurait préféré ne pas revoir de sitôt Flavio D. Garcia. Travaillant à l'université de Birmingham, cet ingénieur en informatique présente, lors de la conférence Usenix qui se tient du 10 au 12 août à Austin (Texas), les conclusions d'une étude (« Lock it and still lose it ») sur les télécommandes permettant l'ouverture des voitures de tourisme.

Des conclusions peu flatteuses pour le groupe automobile allemand : la quasi-totalité des véhicules qu'il a vendus ces 20 dernières années, près de 100 millions pour la seule période allant de 2002 à 2015, peuvent être déverrouillés sans clés… et sans plip, du nom de cette fameuse télécommande aujourd'hui livrée en standard avec la plupart des voitures de tourisme.

Flavio D. Garcia étudie depuis plusieurs années les vulnérabilités associées aux systèmes de commande à distance dans l'univers automobile. En 2012, il avait constaté, avec plusieurs collègues, que les récepteurs RFID Magamos Crypto, adoptés par de nombreuses marques de luxe, pouvaient être détournés non seulement pour ouvrir et fermer les portes, mais aussi pour faire démarrer le moteur, le tout sans disposer des clés.

Contacté par ses soins en mai 2013, Volkswagen avait déposé plainte, arguant qu'une publication de ces recherches exposerait ses véhicules à un risque accru de vol. La Haute Cour du Royaume-Uni lui avait accordé une injonction, retardant d'autant la publication, finalement effectuée il y un an et sous une forme très restreinte : une seule phrase, dans les annexes de la conférence Usenix, comme le souligne *Bloomberg*.

Arduino pour intercepter les données

Cette fois-ci, Flavio D. Garcia s'est épargné les considérations juridiques. Avec deux associés de l'université de Birmingham et la firme allemande Kasper & Oswald, il aborde deux vulnérabilités distinctes ; l'une concernant Volkswagen et l'autre applicable à une longue liste de constructeurs.

Point commun entre ces failles : elles sont fondées sur l'interception des données transmises par les télécommandes, qui fonctionnent sur les bandes de fréquence à 433 ou 868 MHz en Europe et 315 MHz en Amérique du Nord – à l'exception de quelques anciens systèmes basés sur la technologie infrarouge.

Le module d'interception, sur base Arduino.

Pour intercepter les données envoyées par les télécommandes, les chercheurs ont fabriqué un module radio à partir d'une carte Arduino. Et se sont aperçus que, de manière générale, le niveau de protection des données dépendait de l'âge des véhicules. Sur des modèles du début des années 2000, il arrive qu'aucune méthode de cryptographie ne soit appliquée : un code unique est envoyé à chaque appui sur le(s) bouton(s) d'ouverture et de fermeture des portes. Sur des voitures plus récentes, des paramètres ont été ajoutés. Notamment un compteur incrémenté à chaque pression, permettant d'éviter qu'une commande soit exécutée deux fois.

Clonage des clefs

Mais, dans tous les cas, il est possible de déterminer la structure des paquets de données, d'autant plus que ceux-ci sont souvent transmis à plusieurs reprises, sans doute pour s'assurer que la communication aboutisse dans les environnements difficiles sujets à des interférences.

Une télécommande Volkswagen de nouvelle génération.

L'équipe de Flavio D. Garcia a identifié pas moins de 7 schémas de transmission. Parfois, le signal varie en amplitude ; d'autres fois, en fréquence. La quantité de données change elle aussi, au même titre que les algorithmes de chiffrement. Mais dans tous les cas, la sécurité peut être déjouée et la clé, clonée.

Cette opération de clonage ne peut toutefois se faire qu'une fois obtenue la clé logée dans le récepteur RFID de la voiture. Pour cela, les chercheurs en ont extrait le *firmware*. Et ont alors fait une sacrée découverte : cette « clé maîtresse » est la même sur des dizaines de millions de véhicules du groupe Volkswagen.

Mais aussi Nissan, Dacia, et Renault…

Sur la liste – non exhaustive – des modèles considérés comme vulnérables figurent les Audi A1, Q3, R8, S3 et TT, les Skoda City Go, Roomster, Fabia 1 et 2, Octavia, SuperB et Yeti, les Seat Alhambra, Altea, Arosa, Cordoba, Ibiza, Leon, MII et Toledo… ainsi que les Volkswagen Amarok, (New) Beetle, Bora, Caddy, Crafter, e-Up, Eos, Fox, Golf 4, 5 et 6, Golf Plus, Jetta, Lupo, Passat, Polo, T4, T5, Scirocco, Sharan, Tiguan, Touran et Up.

Dans le prolongement de ces conclusions, Flavio D. Garcia et consorts se sont intéressés aux circuits intégrés PCF7946 et PCF7947, que le fabricant de semi-conducteurs NXP fournit à de nombreux constructeurs automobiles, détaillent nos confrères de *ITespresso*.

Avec le même mode opératoire, ils sont ainsi parvenus à pirater une Fiat Punto, un Citroën Jumper, un Dacia Duster, une Renault Modus ou encore un Nissan Qashqai. Il leur a toutefois fallu ici pousser l'expérimentation plus loin, en interceptant plusieurs codes (4 à 8, d'après le rapport, car ces codes changent à chaque pression sur la télécommande) et en utilisant un ordinateur pour déchiffrer certaines données. En l'occurrence, une partie des 28 bits du compteur.

Une étape indispensable : sur un grand nombre de véhicules, la télécommande se bloque si ledit compteur, censé augmenter d'une unité à chaque appui, n'est pas synchronisé avec celui du récepteur RFID.

Des vols bien réels

Le déchiffrement prend moins de 10 minutes en exploitant les failles de HiTag2, un algorithme de cryptographie lancé il y a près de 20 ans et associé aux circuits intégrés PCF7946/7947. Pour intercepter plus rapidement le nombre de codes requis, les chercheurs ont bloqué la transmission des signaux afin que les utilisateurs ciblés pressent à nouveau le bouton de leur télécommande.

La principale limitation de la méthode imaginée par les chercheurs réside dans la portée des télécommandes. Généralement quelques dizaines de mètres. Il faut donc impérativement se trouver dans ce périmètre. Dès lors, il est possible d'envisager d'autres scénarios d'attaque. Par exemple, une sorte de DDoS à partir du système de blocage de la télécommande.

Ces recherches permettent de mettre le doigt sur un phénomène en pleine explosion : aux États-Unis, les forces de l'ordre constatent de plus en plus de vols de voitures sans effraction. Les images de vidéosurveillance révèlent souvent l'utilisation d'un simple boîtier électronique. Ce mois-ci, une trentaine de Jeep ont ainsi été volées dans le Texas avec un simple ordinateur.

Article original de Silicon

Original de l'article mis en page : Sécurité : toutes les Volkswagen peuvent être ouvertes sans clef

---

« AITEX – AFRICA IT EXPO » : le Sénégal et la Côte d'Ivoire à l'honneur au Maroc, du 21 au 24 septembre 2016

« AITEX – AFRICA IT EXPO » : le Sénégal et la Côte d'Ivoire à l'honneur au Maroc, du 21 au 24 septembre 2016

Le Sénégal et la Côte d'Ivoire, qui compte parmi les pays d'Afrique subsaharienne à avoir engagé des projets de gouvernance électronique, seront à l'honneur au Maroc lors de la première édition du Salon de l'innovation et de la transformation digitale en Afrique, « AITEX – AFRICA IT EXPO », qui aura lieu du 21 au 24 septembre 2016 à Casablanca.

Dans un communiqué transmis à notre Rédaction, la **Fédération marocaine des technologies de l'information, des télécommunications et de l'Offshoring (APEBI),** chef d'orchestre de l'AFRICA IT EXPO, explique le choix du Sénégal et de la Côte d'Ivoire par le souci d'établir une connexion sud-sud des ressources du continent. Un défi majeur que le Royaume chérifien veut relever en commençant par ces deux pays qui sont la locomotive économique de la sous-région ouest-africaine. La Côte d'Ivoire connaît une forte croissance économique qui se situe entre 7 et 8 % par an. Une performance portée en partie par un secteur privé qui fait de la transformation numérique, un vecteur de compétitivité. Le Sénégal, deuxième économie de l'Afrique de l'Ouest francophone derrière la Côte d'Ivoire, est plébiscitée pour les efforts fournis dans le domaine du digital. Là où l'Afrique a atteint un taux de pénétration moyen autour de 100%, le Sénégal lui signe un taux de 113,66% en mars 2016. En choisissant ces deux pays, le Maroc veut leur apporter son « soutien pour conforter leur leadership régional et aussi pour accélérer leur transformation numérique ».

Le communiqué :
« Salon des Technologies de l'Information « AITEX – AFRICA IT EXPO » – 21 – 24 septembre 2016 à Casablanca
Le 1er salon de l'innovation et de la transformation digitale du continent met à l'honneur le Sénégal et la Côte d'Ivoire

La Fédération marocaine des technologies, de l'information, des télécommunications et de l'Offshoring (APEBI) organise la 1ère édition du Salon des Technologies de l'Information « AITEX – AFRICA IT EXPO », qui aura lieu du 21 au 24 septembre 2016 à la foire internationale de Casablanca. « AITEX – AFRICA IT EXPO » est la première plateforme de l'innovation et de la transformation digitale en Afrique, qui va réunir 150 exposants – tous issus des entreprises référencées dans le domaine -, 200 donneurs d'ordre, mais aussi des experts et des utilisateurs venus d'Afrique, du Moyen Orient et d'Europe. Pour cette édition, l'APEBI met à l'honneur le Sénégal et la Côte d'Ivoire, deux pays amis avec lesquels le Royaume entretient des relations de longue date, qui constituent un modèle de coopération exemplaire, et qui jouent par ailleurs un rôle de locomotive en Afrique de l'Ouest dans le domaine des TIC.

Aujourd'hui, la transformation digitale est devenue un enjeu majeur pour les sociétés, une mutation indispensable pour les entreprises et l'économie. A l'ère du numérique, cette transformation constitue un avantage fort pour nos sociétés, qui crée de la valeur… L'évolution très rapide des TIC -Technologies de l'Information et de la Communication- a profondément façonné le changement de nos modes de vie. Face à la généralisation des TIC dans les pays industrialisés, l'intégration de ces compétences (mais surtout leur maîtrise et leur exploitation) est un enjeu stratégique, sociétal, culturel et technologique en Afrique.
Le continent, qui poursuit son processus de mondialisation et sa dynamique d'émergence doit se « mettre à niveau » pour améliorer l'efficience de son économie et « booster » sa compétitivité locale et internationale. Grâce à une approche bien encadrée, qui va intégrer tous les paramètres, les enjeux et aussi les risques induits, la transformation digitale est sans conteste un levier de croissance économique et de compétitivité, créateur de valeur ajoutée.
La Fédération marocaine des technologies, de l'information, des télécommunications et de l'Offshoring (APEBI), est un acteur régional stratégique en Afrique car elle regroupe des entreprises qui jouent un rôle clé dans l'économie et qui sont des références dans leur domaine.
Pendant trois jours, l'APEBI va être le catalyseur d'une dynamique nouvelle, qui va accélérer le développement du numérique dans le continent.

AITEX – AFRICA IT EXPO : Première plateforme de l'innovation et de la transformation digitale d'Afrique
Cette édition sera marquée par une forte présence d'experts de haut niveau, des opérateurs nationaux et internationaux reconnus, tous réunis autour d'un programme ambitieux qui a pour vocation d'être la première plateforme de l'innovation et de la transformation digitale en Afrique.
Organisé avec le soutien institutionnel de Maroc Export, le salon « AITEX – AFRICA IT EXPO » va accueillir principalement des distributeurs, des fournisseurs de technologie, des intégrateurs de solutions, éditeurs, opérateurs télécoms, ISP, ASP, délocalisation de fonctions de gestion, TMA, help desk conseil, offshoring, mobility, big data, Cloud, réseaux, e-Commerce… Vitrine de l'offre numérique et des dernières évolutions digitales, « AITEX – AFRICA IT EXPO » est une *plateforme* unique de rencontres, d'échanges et d'opportunités d'affaires.
Véritable révélateur des nouvelles tendances, le Salon «AITEX – AFRICA IT EXPO » est une occasion unique de rencontrer et d'échanger sur les problématiques quotidiennes des entrepreneurs, collectivités et de trouver les réponses appropriées grâce au concours de spécialistes, eux-mêmes engagés dans les processus de développement des économies émergentes et de la coopération sud-sud.
Placé sous le thème, «Transformation Digitale : Levier de développement en Afrique», le salon offre une nouvelle occasion de conscientiser et sensibiliser nos sociétés sur la formidable opportunité offerte par les technologies numériques pour accélérer le développement du continent. Des rencontres sont organisées au cours de ces trois journées pour débattre des problématiques actuelles et des enjeux sociétaux de ces mutations afin d'adopter les meilleures pratiques et ainsi anticiper les défis auxquels les entreprises et économies africaines sont confrontées.
«AITEX – AFRICA IT EXPO » va promouvoir les relations d'affaires et la mise en réseau des différents acteurs économiques du continent, à travers des coopérations sud-sud, nord-sud et public-privé.

Le Sénégal et la Côte d'Ivoire à l'honneur
Le défi numérique en Afrique passe inéluctablement par la connexion des ressources du continent. Un aspect *que l'APEBI a compris et intégré dans l'organisation de ce salon, c'est pourquoi la fédération a décidé de mettre à l'honneur, pour sa première édition, le Sénégal et la Côte d'Ivoire.* Ces deux pays, représentant deux premières puissances économiques de l'Afrique de l'ouest francophone engagés dans une dynamique de croissance depuis plusieurs années, ont à cœur de poursuivent respectivement leurs ambitions numériques.
La Côte d'Ivoire connaît une forte croissance économique qui se situe entre 7 et 8 % par an et le développement du numérique est devenu un enjeu majeur, créateur de richesses. Le numérique constitue un potentiel énorme, présent dans tous les esprits, aussi bien du côté du gouvernement que des dirigeants d'entreprise. Selon une étude publiée par le cabinet Deloitte en mai 2016, seulement 36 % des entreprises estiment avoir atteint la maturité numérique.
Le Sénégal, quatrième économie de la sous-région ouest africaine après le Nigéria, la Côte d'Ivoire et le Ghana, et deuxième économie en Afrique de l'Ouest francophone derrière la Côte d'Ivoire s'est largement distingué dans l'évolution de l'économie numérique, premier levier de la transformation digitale. Là où l'Afrique a atteint un taux de pénétration moyen autour de 100%, le Sénégal lui signe un taux de 113,66% en mars 2016.
Le *Sénégal et la Côte d'Ivoire font partie des premiers pays africains à initier des* projets de gouvernance électronique (e-Gouv). Ils ont réalisé au fil des années des progrès importants dans les domaines tels l'économie numérique, la monétique, le courrier hybride, ou encore le taux de connectivité internet, etc.) Néanmoins, les disparités qui existent entre les différents pays du continent peuvent être réduites si un effort de coopération est accompli.
En mettant en avant ces deux pays amis, qui constituent un modèle important d'exemplarité sur le continent africain (et en particulier de ses voisins ouest-africains), le Maroc apporte son soutien pour conforter leur leadership régional et aussi pour accélérer leur transformation numérique. »
Article original de Cio-Mag

Original de l'article mis en page : « AITEX – AFRICA IT EXPO » : le Sénégal et la Côte d'Ivoire à l'honneur au Maroc, du 21 au 24 septembre 2016 | CIO MAG