Cybercriminalité : « Il faut qu’on voie que la Côte d’Ivoire réagit » | CIO MAG

Cybercriminalité : « Il faut qu’on voie que la Côte d’Ivoire réagit »

« L'enjeu qu'a la Côte d'Ivoire aujourd'hui, c'est justement de dire de manière internationale tout ce qu'elle est en train de mettre en œuvre ici », assure Denis Jacopini, expert informatique assermenté spécialiste en cybercriminalité et protection des données personnelles. Membre de la Compagnie nationale française des experts de Justice en Informatique et techniques associées (CNEJITA), il a participé du 7 au 8 juin 2016 à Abidjan, à la 8ème édition de l'IT Forum Côte d'Ivoire sur la « Transformation numérique face à la protection des utilisateurs ». Loin des clichés et des idées reçues, le professionnel du crime en ligne a confié à CIO Mag l'image que la Côte d'Ivoire donne de l'extérieur et fait des propositions allant dans le sens de l'amélioration de la lutte contre la cybercriminalité. Sensibilisation des décideurs, opérations coup de poing, médiatisation des arrestations… la Côte d'Ivoire est, selon lui, en bonne voie pour renforcer la confiance dans son environnement numérique.

7 juin 2016. Denis Jacopini à la 8ème édition de l'IT Forum Côte d'Ivoire qui s'est déroulée du 7 au 8 juin dernier à la Maison de l'Entreprise, à Abidjan, sur le thème : « Transformation numérique face à la protection des utilisateurs ».

CIO Mag : Quelle image la Côte d'Ivoire donne-t-elle de l'extérieur dans le domaine de la cybercriminalité ?
Denis Jacopini : Depuis quelques années, la Côte d'Ivoire est connue en Europe comme le pays d'Afrique où se passent la très grande majorité des arnaques sur internet, à un point où lorsque quelqu'un reçoit un email qui vient de Côte d'Ivoire, il pense automatiquement à une arnaque, au mieux se méfie, au pire supprime le message sans même lui accorder la moindre attention. Ainsi, associer la Côte d'Ivoire à des arnaqueurs, n'est pas bon pour l'image du pays. Ceci dit, ma présence ici m'a réconforté.
En lisant la presse spécialisée, dont CIO Mag, je savais déjà que la Côte d'Ivoire réagissait face à ce phénomène, qu'elle mettait en place des méthodes et qu'elle engageait des actions pour permettre à la fois aux directeurs de systèmes d'information – DSI – et aux utilisateurs d'augmenter en compétence et de se soucier de ce problème de sécurité. Et, en venant ici, ça m'a réconforté. Je m'en suis surtout rendu compte au travers du discours du ministre de l'Economie numérique et de la Poste (à l'ouverture de la 8ème édition de l'IT Forum Côte d'Ivoire, NDLR). Il a fait une présentation de la manière dont il voit l'évolution de la Côte d'Ivoire dans le domaine du numérique. Son discours a été rassurant en indiquant que le pays avait à la fois une démarche active dans la cybersécurité et accordait une attention particulière aux moyens permettant d'associer confiance et développement numérique.
On a facilement pu remarquer que le ministre maîtrise le sujet et qu'il sait de quoi il parle. Il est prêt à emmener avec lui le pays dans cette transformation numérique. Quasiment toutes les entreprises vont devoir assurer cette métamorphose. Le pays doit pouvoir les accompagner dans cette transformation numérique. L'enjeu qu'a la Côte d'Ivoire aujourd'hui, c'est justement de dire de manière internationale tout ce qu'elle est en train de mettre en œuvre ici.

C.M : Selon vous quels sont les actions sur lesquelles la Côte d'Ivoire doit miser pour véritablement restaurer son image et créer un environnement numérique de confiance ?
D.J : A mon avis, ça devrait passer par une médiatisation des arrestations. Il y a des milliers de délinquants ayant organisé et mené des arnaques en tous genres à partir de cybercafés. On apprend de temps en temps sur la presse francophone spécialisée que se sont produites des arrestations mais ça reste sur les journaux peux lus. Il faut vraiment s'intéresser à la Côte d'Ivoire et consulter la presse locale pour le savoir. A mon avis, les actions qui sont faites dans le pays mais aussi tous les accords et toutes les coopérations qui sont établis avec les autres pays doivent internationalement être connues et notamment par le grand public qui a besoin d'être rassuré car régulièrement victime d'actes originaires d'ici.
Lorsqu'il y a une coopération qui est mise en place avec l'ANSSI (l'Agence nationale de la sécurité des systèmes d'information, NDLR) en France, avec l'OCLCTIC, l'Office centrale de lutte contre la criminalité liée aux technologies de l'information et de la communication, en termes de formation et de sensibilisation en Côte d'Ivoire, il faut que cela se sache. Il faut qu'on voie que la Côte d'Ivoire réagit que les autorités se forment, sont en train de monter en compétence. Maintenant, ce qui manque, ce sont les preuves. Mais les preuves, ce sont effectivement les statistiques pouvant faire mention de l'évolution du nombre d'arrestations que j'espère suivies d'une chute considérable des arnaques qui pourraient venir rassurer les pays victimes. Il y aura toujours des arnaques, mais celles venant de Côte d'Ivoire doivent être combattues sans cesse pour finir par les rendre anecdotiques.

C.M : Hormis les arrestations, une forte sensibilisation de la jeunesse ivoirienne ne peut-elle pas également contribuer à réduire le nombre d'arnaques venant de la Côte d'Ivoire ?
D.J : D'après ce que j'ai compris, les adolescents ou les jeunes qui sont concernés sont des personnes qui, dans la société, sont déjà en marge des règles. Ils essaient de se débrouiller par leurs propres moyens sans passer par la case Travail, la case Honnêteté. C'est tout aussi grave que de se rapprocher de la drogue. Que fait le pays contre la drogue ? Ce qu'elle fait contre ce fléau, elle doit aussi le faire pour combattre la cybercriminalité. Comme dans d'autres régions du monde, s'attaquer à ce phénomène doit se faire en s'appuyant sur des entraides internationales.
« CE QUI MANQUE MAINTENANT CE SONT LES MOYENS POUR LES POUVOIRS PUBLICS DE MENER DES OPÉRATIONS COUP DE POING. GRÂCE À CELA, IL EST PROBABLE QUE LES JEUNES POUVANT ENCORE CHANGER DE VOIE, LE FERONT PAR PEUR.»
L'analyse des flux financiers au travers de réseaux et des trains de vie incohérents avec les revenus connus sont de bonnes pistes à suivre pour comprendre le phénomène de la cybercriminalité. Ce qui manque maintenant ce sont les moyens pour les pouvoirs publics de mener des opérations coup de poing. Grâce à cela, il est probable que les jeunes pouvant encore changer de voie, le feront par peur. Ensuite, pour ceux qui, influencés, n'auront pas envie de rentrer dans le droit chemin, je pense en effet qu'une une forte sensibilisation pourra évidemment contribuer à réduire le nombre d'arnaques venant de Côte d'Ivoire.

C.M : Parlant de moyens, n'est-il pas opportun de renforcer la coopération avec la France et des pays comme le Canada pour muscler les opérations terrain, ce d'autant plus que les populations de ces pays sont bien souvent ciblées par les arnaques venant de Côte d'Ivoire ?
D.J : Jusqu'à maintenant, la coopération n'y était pas. Elle était surtout en Europe. En dehors de l'Europe, c'était très difficile d'établir une coopération. Moi, il y a une question que je me pose : pourquoi d'ici ils vont essayer d'arnaquer la France ou le Canada ? Déjà parce qu'il n'y a pas de barrière au niveau de la langue. Puis, ce sont des pays qui ont des moyens. Qui sont prêts à payer pour rencontrer l'amour. On ne va pas essayer d'arnaquer un pays pauvre. Donc, on s'oriente vers ces pays-là.
Depuis maintenant quelques années, au-delà de l'évolution de la législation, la coopération internationale entre pays intérieurs et extérieurs de l'Europe s'est accentuée. Sans que ces pays n'aient forcément ratifié la Convention de Budapest, seul contrat officiel existant et contenant des protocoles d'entraides entre les autorités compétentes des différents pays impliqués, une entraide entre les organes judiciaires s'est naturellement créée. Aujourd'hui, l'entraide internationale est légion. C'est une forme de coopération qui n'a pas besoin de convention et qui, avec certains pays fonctionne très bien. En partie grâce à cela, la Côte d'Ivoire a commencé ces dernières années à s'attaquer au délinquants du numérique, réaliser des arrestations et amplifier ses actions…

C.M : Vous avez participé à l'IT Forum Côte d'Ivoire 2016 sur la sécurité des utilisateurs des services numériques. Partant de tout ce qui a été dit, comment entrevoyez-vous l'avenir de la Côte d'Ivoire dans 5 à 10 ans ?
D.J : La Côte d'Ivoire est en bonne voie pour sortir la tête de la cybercriminalité. Elle est en bonne voie parce que le combat commence obligatoirement par la sensibilisation des décideurs. Et ce forum a réuni des DSI, des directeurs de la sécurité numérique, des chefs d'entreprises, des officiels, donc des personnes qui décident de l'économie du pays. Si, nous formateurs, consultants, professionnels de la cybersécurité, on a bien fait notre travail pendant ces deux jours, il est clair que les visiteurs sont repartis d'ici avec de nouvelles armes. Maintenant, ceux qui auront été convaincus aujourd'hui ne seront pas forcément ceux qui seront les cibles de demain, des prochaines failles ou des prochaines attaques. Les prochaines victimes continueront à être les utilisateurs imprudents, ignorants et des proies potentielles qui n'ont pas pu être présentes à l'IT Forum. À force de sensibiliser les chefs d'entreprises, les DSI, et de faire en sorte que la sensibilisation à la cybersécurité et aux comportements prudents commence dès l'école, nous auront bientôt une nouvelle génération d'utilisateurs mieux formés et mieux armés.
Un autre phénomène qui tend à être inversé est celui de la faible importance accordée à la sécurité informatique. Quel que soit l'endroit dans le monde, la cybercriminalité est quelque chose d'inévitable et la sécurité informatique, en raison d'une course effrénée à la commercialisation à outrance, a trop longtemps été négligée par les constructeurs et les éditeurs de logiciels. Ils devront sans doute se conformer au concept « Security by design ».
Avant de miser sur sa R&D (Recherche et Développement) pour créer ou répondre à des besoins et commercialiser à tout prix pour rapidement la rentabiliser et ne chercher que les profits financiers, il deviendra bientôt obligatoire de penser sécurité avant de penser rentabilité. Avec l'évolution incoercible du numérique dans notre quotidien (objets connecté, santé connectée, vie connectée), il est indispensable que la sécurité des utilisateurs soit aussi le problème des inventeurs de nos vies numériques et pas seulement de ceux dont le métier est de réparer les bêtises des autres. La Côte d'Ivoire fait désormais partie des pays impliqués par ce combat et je n'ai aucun doute, ce pays se dirige droit vers une explosion de l'usage du numérique et une amélioration de sa lutte contre la cybercriminalité.

C.M : Au niveau international, quelle est la nouvelle tendance en matière de cybercriminalité?
D.J : Au Forum international de la cybercriminalité (FIC 2016), j'ai assisté à une présentation faite par un chercher en cybersécurité autour de l'étude de l'évolution d'un RAT (Remote Access Tool). Des virus utilisant des failles existent déjà mais la présentation portait sur une nouvelle forme de logiciel malveillant encore plus perfectionné en matière d'impacts et de conséquences sur les postes informatiques des victimes. On connaissait des failles en Flash, en Visual Basic et dans d'autres types de langages mais la faille en Java est une faille qui aujourd'hui peut toucher tous les ordinateurs puisqu'énormément de systèmes et de web services sont conçus autour du langage Java.
J'ai trouvé la présentation très intéressante et j'ai trouvé l'effet dévastateur pour tous ceux qui attraperont ce « Méchangiciel ». A la fin de la présentation, j'ai approché l'intervenant et lui ai demandé quel était le moyen de propagation utilisé par ce virus ingénieux du futur ? Il m'a répondu qu'il se propage tout simplement par pièce jointe dans un e-mail. Ça reste aujourd'hui le principal vecteur de propagation de systèmes malveillants. Surtout, si c'est bien monté avec ce qu'on appelle des techniques d'ingénierie sociale, c'est-à-dire des actes qui permettent de manipuler la personne destinataire du piège, par exemple un CV piégé transmis à une agence d'emploi, rien de plus normal, même s'il est piégé ! C'est pourquoi l'autre vecteur sur lequel j'insiste, c'est le vecteur humain, la sensibilisation des utilisateurs afin d'augmenter le taux de prudence qu'ils doivent avoir lorsqu'ils reçoivent un email. Un email piégé a des caractéristiques que l'on peut assez facilement identifier et qui permettent de dire qu'il y a un risque, et mettre une procédure en cas de doute. Pour moi, même s'il existe des lunettes 3D, des hologrammes, des choses complétement folles au niveau technologique, j'ai l'impression que la propagation de la cybercriminalité va pouvoir se faire encore pendant pas mal de temps dans de vulgaires pièces jointes, et probablement encore dans les arnaques et le phishing.
Une fois que le pirate aura obtenu les clefs il pourra mener son attaque par « Menace Persistante Avancée (Advanced Persistent Threat) », autre grande tendance déjà depuis quelques années et encore pour longtemps !
Article original et propos recueillis par Anselme AKEKO

Réagissez à cet article

Original de l’article mis en page : Cybercriminalité : « Il faut qu’on voie que la Côte d’Ivoire réagit » | CIO MAG

Vidéo sur l’étude du marché de la cybersécurité par Xerfi

	**Vidéo sur l’étude du marché de la cybersécurité par Xerfi**

La cybersécurité est l'un des marchés les plus dynamiques de l'IT, d'après l'étude de Xerfi sur le sujet. Il faut dire que les soutiens à l'activité sont nombreux entre la recrudescence des menaces informatiques, la mise en place de nouvelles réglementations plus contraignantes et les nouvelles vulnérabilités liées aux évolutions des techniques et des pratiques […]

Article original de Alexandre Boulègue

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 : Alexandre Boulègue, Xerfi – Le marché de la cybersécurité – Secteurs & marchés – xerficanal-economie.com

---

Russie : Edward Snowden dénonce une loi « Big Brother » et la « surveillance de masse » en Russie

	Edward Snowden dénonce une loi « Big Brother » et la « surveillance de masse » en Russie

Edward Snowden, l'ancien agent du renseignement américain réfugié en Russie, a dénoncé samedi 25 juin les lois antiterroristes adoptées par les députés russes. Ces dernières relèvent selon lui de « Big Brother » et de la « surveillance de masse », et a demandé qu'elles ne soient pas promulguées.

« La nouvelle loi russe Big Brother constitue une violation inapplicable et injustifiable des droits qui ne devrait jamais être promulguée », a écrit sur Twitter le lanceur d'alerte, qui a fui les Etats-Unis pour révéler l'ampleur de la surveillance menée par les services de renseignement américains.
« La surveillance de masse ne marche pas. Ce texte va coûter de l'argent et de la liberté à chaque Russe sans améliorer la sécurité », a-t-il insisté dans un second message.

Des lois extrêmement répressives

Adoptés vendredi lors de la dernière séance de la Douma (chambre basse) avant les législatives du 18 septembre, les projets de loi en question obligent en particulier les opérateurs de télécommunications et internet à stocker les messages, appels et données des utilisateurs pendant six mois pour les transmettre aux *« agences gouvernementales appropriées »* à leur demande.
Les réseaux sociaux se voient également obligés de stocker les données pendant six mois, selon l'un de ces textes qui doivent encore être approuvés par le Conseil de la Fédération (chambre haute) et promulgués par M. Poutine.
Ce délai de six mois *« n'est pas seulement dangereux, il est inapplicable »*, a prévenu M. Snowden, qui avait été critiqué, par le passé, pour ne pas critiquer assez sévèrement le régime de Vladimir Poutine.
Ces lois ont été dénoncées par l'opposition russe comme une tentative de *« surveillance totale »* de la part des autorités, mais aussi par les entreprises du numérique qui ont critiqué un coût exorbitant.
Elles introduisent par ailleurs des peines de prison pour la non-dénonciation d'un délit, abaissent l'âge de la responsabilité pénale à 14 ans et introduisent des peines allant jusqu'à sept ans de détention pour la*« justification publique du terrorisme »*, y compris sur internet.
Article original Le Monde

Réagissez à cet article

Original de l'article mis en page : Russie : Edward Snowden dénonce une loi « Big Brother » et la « surveillance de masse »

Bulletin sécurité du 13 juin 2016 du CERTFR

Bulletin sécurité du 13 juin 2016 du CERTFR

La S . G . D . S . N (Agence nationale de la sécurité des systèmes d'information) met régulièrement à notre disposition ses avis et alertes sur de nouvelles vulnérabilités détectées.
Voici le dernier bulletin d'actualité : CERTFR-2016-ACT-024

1 – Sonde de détection d'intrusions réseau – Comment implémenter les points de mesure ?

Une sonde de détection d'intrusions réseau est un équipement passif, elle ne s'insère donc pas en coupure sur un flux de production. Il est donc nécessaire, pour implémenter les points de mesure définis, d'assurer une duplication en temps réel de l'activité réseau à analyser.
Deux techniques différentes existent pour dupliquer un trafic réseau : la première, généralement appelée « port miroir », est logicielle, et s'appuie sur les équipements réseau déjà en place ; la seconde, généralement appelée « tap », s'appuie sur des boîtiers matériels dédiés à cette fonction. Nous allons voir les avantages et les inconvénients de ces deux solutions.

Port miroir

La majorité des commutateurs du marché permettent de configurer une recopie logicielle de tout ou partie du trafic sur un ou plusieurs ports physiques dédiés. Le port miroir peut être un choix peu coûteux, si les équipements existants d'un réseau disposent déjà de cette fonctionnalité.
Toutefois, la recopie logicielle du trafic n'est pas sans risque. En effet, si l'équipement atteint sa limite de capacité sur ses fonctions « principales » (comme par exemple : la commutation de paquets, le routage, etc.), des fonctions annexes comme la recopie de paquets peuvent être dégradées, entraînant dans un tel cas des pertes sur l'activité à superviser.
La recopie logicielle peut également altérer le signal, car les couches basses réseau sont analysées et traitées par les commutateurs. Cette technique ne garantit donc pas la recopie de l'intégralité du trafic commuté sur le réseau de production. Étant donné qu'un seul paquet perdu sur un flux volumineux peut empêcher l'analyse par la sonde ou l'évader, il est primordial de considérer ce problème et de superviser la charge des commutateurs, si cette technique est mise en place.
La mise en place d'un port miroir sur un équipement du réseau augmente aussi la consommation de ressources : cela peut donc également dégrader le réseau de production. Une attention particulière doit être apportée au fond de panier, car le débit total commuté par l'équipement est décuplé.
D'autre part, il est important d'intégrer les ports miroirs dans les procédures d'exploitation : lors du remplacement d'un équipement ou d'un changement de configuration, il faut s'assurer que la recopie est toujours opérationnelle et qu'il n'y a pas de perte d'une partie des flux.
Une erreur de configuration peut également autoriser des communications depuis le réseau de duplication, voire même entre la sonde et le réseau de production.
Par contre, la mise en oeuvre d'un port miroir peut se faire sans interruption du réseau en production à superviser, à condition de disposer de suffisamment de ports physiques libres au niveau des commutateurs où les points de mesure sont effectués.

TAP

Un TAP garantit la recopie stricte du signal reçu : aucune analyse des couches au-delà de celle physique n'est réalisée. Le signal est régénéré électriquement pour des TAP cuivre, et la lumière est divisée sur deux chemins pour les TAP fibre. La mise en oeuvre d'une duplication de trafic sur un réseau en production nécessite une brève interruption du lien à superviser : celle-ci correspond au temps nécessaire pour placer le boîtier TAP en « coupure », c'est-à-dire sur le chemin de câble.
Pour les TAP alimentés, un défaut d'alimentation arrête la duplication, mais le TAP reste passant pour le lien coupé, moyennant généralement une microcoupure de quelques millisecondes.
Pour les TAP fibre, une partie de la lumière incidente étant réfléchie et l'autre réfractée, le signal est affaibli en fonction de proportions précisées dans la documentation du TAP.
Contrairement au port miroir, le TAP garantit également l'isolation entre le réseau de production et le réseau de détection.
Le prix d'un boîtier de duplication de trafic (TAP) varie entre une centaine d'euros et un millier, en fonction du type de média à dupliquer.

Conclusion

En conclusion, bien que ces deux méthodes permettent la duplication du trafic, il est conseillé de privilégier l'utilisation d'équipement dédié afin de garantir la séparation entre le réseau de production et le réseau de détection, ainsi qu'une recopie à l'identique des flux réseau.

2 – Rappel des avis émis

Dans la période du 06 au 12 juin 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-190 : Vulnérabilité dans VLC Media Player
- CERTFR-2016-AVI-191 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2016-AVI-192 : Multiples vulnérabilités dans Wireshark
- CERTFR-2016-AVI-193 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2016-AVI-194 : Multiples vulnérabilités dans les produits Symantec
- CERTFR-2016-AVI-195 : Multiples vulnérabilités dans PHP
- CERTFR-2016-AVI-196 : Multiples vulnérabilités dans SCADA les produits Siemens
- CERTFR-2016-AVI-197 : Vulnérabilité dans Citrix Xenserver
- CERTFR-2016-AVI-198 : Multiples vulnérabilités dans les produits VMware
- CERTFR-2016-AVI-199 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

---

Réagissez à cet article

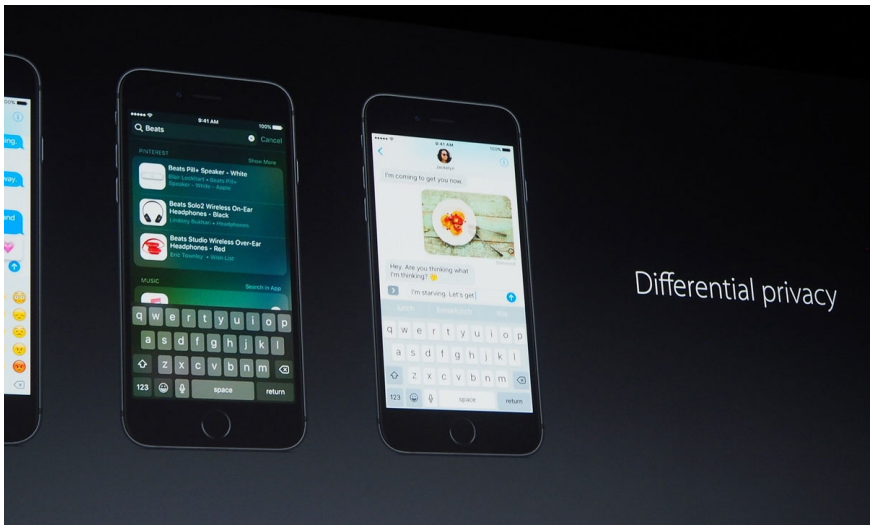
Original de l’article mis en page : Bulletin d’actualité CERTFR-2016-ACT-024

Finalement Apple collectera des données personnelles, avec votre accord

Finalement Apple collectera des données personnelles, avec votre accord

---

Point d'achoppement et de différence avec Google, Facebook et autres, votre vie privée et les données qui y sont associées sur vos appareils n'intéressent pas Apple.Jusqu'alors, Apple s'est toujours refuser à accéder ou collecter vos données.



Point d'achoppement et de différence avec Google, Facebook et autres, votre vie privée et les données qui y sont associées sur vos appareils n'intéressent pas Apple.
Jusqu'alors, Apple s'est toujours refuser à accéder ou collecter vos données.
Cependant les nouvelles fonctionnalités de suggestion et d'identification d'iOS 10 ne peuvent se prétendre pertinentes sans avoir accès à un minimum de données !
Les techniques de « differential privacy » mises en oeuvre pour iOS 10 ne permettront pas une identification de l'utilisateur qui fournit ses données mais Apple, selon Recode, vous- demandera votre accord avant d'attaquer toute collecte d'information.
Dans un premier temps, le type de données collectées sera limité à quatre domaines :
– les nouveaux mots ajoutés au dictionnaire personnel d'iOS,
– les émoticônes utilisées,
– les liens profonds marqués comme public dans les applications,
– les suggestions de recherche dans les notes.
Pour ne pas rater le train de l'intelligence artificielle, Cupertino ne pouvait pas rester à l'écart d'une forme de collecte et d'exploitation de données. Cependant, ne souhaitant pas en faire directement commerce ni renier ses grands principes, Apple se doit de naviguer entre deux eaux et d'innover dans ce domaine.
On est encore loin de la façon de procéder de compagnies comme Google et Facebook !
Article original de bpepermans

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 : Finalement Apple collectera des données personnelles, avec votre accord | Slice42

Alerte ! Un nouveau malware infecte plus de 850.000 terminaux Android

	Alerte ! Un nouveau malware infecte plus de 850.000 terminaux Android

---

Particulièrement actif en Asie, ce malware est notamment parvenu à se frayer un chemin jusqu'au Google Play Store.

Android a pourtant initié depuis plusieurs années un grand nettoyage de son Google Play Store et a revu les règles et procédures d'accès des applications, mais certains malwares parviennent encore à contourner les garde-fous mis en place. Trend Micro alerte ainsi sur une famille de malware baptisés Godless, qui sont distribués entre autres via le Google Play Store et des applications malveillantes.

Trend Micro explique que Godless dispose de plusieurs exploits lui permettant d'affecter les appareils Android, ce qui le rend potentiellement dangereux pour tous les téléphones disposant d'une version antérieure à Android 5.1.
Le malware est généralement distribué via des applications proposées sur le Google Play store. La présence de celui-ci n'est pas détectée, car lorsque l'application est uploadée vers le playstore, elle ne contient aucun code malveillant à proprement parler. Mais une fois l'application installée, celle-ci va se mettre à jour et télécharger alors le « payload » contenant l'exploit de la vulnérabilité choisie par les cybercriminels.
Le malware tentera d'exploiter celle-ci pour acquérir les droits root sur la machine : il s'en sert par la suite pour installer des applications ou pour diffuser des publicités.
La France est relativement épargnée par ce malware, qui est principalement actif en Asie, notamment en Inde et en Indonésie. Mais Trend Micro estime que plus de 850.000 terminaux Android ont été infectés par ce malware à travers le monde. Outre les applications qui parviennent à le distribuer sur le Google Play Store officiel, celui-ci est évidemment diffusé sur les magasins d'application tiers.
Article original de Louis Adam

Réagissez à cet article

Original de l'article mis en page : Godless : un nouveau malware qui infecte plus de 850.000 terminaux Android – ZDNet

Pourquoi protéger votre connexion sur le Wifi gratuit ?

Pourquoi protéger votre connexion sur le Wifi gratuit ?

Quelques trucs et astuces simples, mais efficaces, pour protéger votre ordinateur, téléphone et tablette.

Wifi gratuit ? Votre meilleur ennemi ! En général, les réseaux Wi-Fi que l'on trouve dans les lieux publics ne sont pas bien protégés. Ils se basent souvent sur des protocoles de chiffrement trop simples ou parfois pas chiffrés du tout. Les pirates peuvent ainsi accéder à chacune des informations que vous envoyez sur Internet : e-mails importants, données de carte bancaire, voire données d'identification permettant d'accéder à votre réseau d'entreprise. Une fois que les pirates disposent de ces renseignements, ils peuvent accéder à vos systèmes en votre nom, diffuser des programmes malveillants, ou facilement installer des logiciels infectés sur votre ordinateur si le partage de fichiers a été activé.

Quelques bons gestes à respecter face à un Wifi gratuit

D'abord, utilisez un réseau privé virtuel (VPN). Un VPN est indispensable lorsque vous accédez à une connexion non sécurisée, comme un point d'accès wifi. Même si un pirate réussit à se placer en plein milieu de votre connexion, les données qui s'y trouvent seront chiffrées, donc illisibles. Mails, mots de passe, ou simplement ce que vous visitez ne seront pas lisibles. J'utilise moi même plusieurs dizaines de VPN différents. Je peux vous proposer de tester Hide My Ass, ou encore VyprVPN. Un test de VPN disponibles pour votre ordinateur, tablette ou encore smartphone dans cet article. Dernier conseil, même si vous ne vous êtes pas activement connecté à un réseau, le matériel wifi équipant votre ordinateur, votre téléphone portable, votre tablette continuent de transmettre des informations. Bref, désactivez la fonctionnalité wifi si vous ne l'utilisez pas.

Activez l'option « Toujours utiliser HTTPS » sur les sites Web que vous visitez fréquemment ou qui nécessitent de saisir des données d'identification. Les pirates ne savent que trop bien que les utilisateurs utilisent les mêmes identifiants et mots de passe pour les forums, leur banque ou leur réseau d'entreprise.

Pour finir, lorsque vous vous connectez à Internet dans un lieu public, via un Wifi gratuit il est peu probable que vous souhaitiez partager quoi que ce soit. Dans ce cas, vous pouvez désactiver les options de partage dans les préférences système. (Kaspersky)

Article original de Damien Bancal

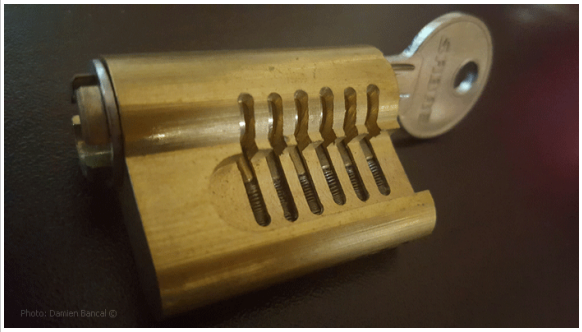
Réagissez à cet article

Original de l'article mis en page : Wifi gratuit, protégez votre connexion – Data Security Breach

Comment devenir maître dans l’art de protéger sa vie privée sur le net ?

Comment devenir maître dans l’art de protéger sa vie privée sur le net ?

Vol de ses données personnelles – Plusieurs sources ont révélé récemment la mise en vente sur le web de plus de 117 millions de profils d'utilisateurs LinkedIn dérobés en 2012. Ce type d'actualité rappelle que personne n'est à l'abri d'un vol de ses données personnelles qui risquent d'être utilisées à des fins illicites. Cette question est d'autant plus cruciale à l'heure où le nombre de logiciels malveillants, ransomwares et autres virus explose. Aujourd'hui, 67 % des Français sont soucieux quant à la protection de leurs informations personnelles sur internet et 83 % d'entre eux sont hostiles à la conservation de ces données (Source : Institut CSA).



Malgré cette méfiance, dans un monde où l'utilisation d'Internet est devenue omniprésente, les utilisateurs ont tendance à exposer très facilement leur vie privée et leurs données personnelles – parfois par paresse ou par mégarde, mais souvent par manque d'information. Il existe cependant des moyens simples et efficaces de limiter ces risques.
Michal Salat, Threat Intelligence Manager chez Avast, commente : « ***Les sphères privées et professionnelles se fondent de plus en plus, poussant fréquemment les utilisateurs à accéder à leurs plateformes de travail depuis des terminaux personnels ou à utiliser leurs appareils professionnels à la maison par exemple. Or, en adoptant ces comportements, les internautes exposent davantage leurs données personnelles.***«

Vol de ses données personnelles
Pour éviter que cela n'arrive, les utilisateurs doivent d'abord se protéger des menaces extérieures à leur appareil en commençant par créer un mot de passe ou un code PIN sur les écrans et les applications mobiles, limitant ainsi l'accès aux données en cas de perte ou de vol. Mais encore faut-il qu'il soit suffisamment compliqué pour ne pas être déchiffré trop facilement. C'est pourquoi il est recommandé d'utiliser des mots de passes complexes – combinant lettres, chiffres, caractères spéciaux et majuscules – et qui ne reprennent pas non plus des informations personnelles facilement accessibles en ligne, telle que la date de naissance ou le prénom de ses enfants. Il est également important de changer ses codes régulièrement.
Il faut garder en tête que les cybercriminels sont à l'affût de la moindre faille à exploiter pour récolter des gains et cherchent très souvent à récupérer des informations bancaires. C'est pourquoi les internautes doivent à tout prix éviter de sauvegarder leurs coordonnées bancaires dans leurs terminaux, quels qu'ils soient. A titre d'exemple, beaucoup d'utilisateurs PayPal ont perdu de grosses sommes d'argent lorsque des hackers ont réussi à se connecter à leurs PC via un compte TeamViewer piraté et se sont servi des identifiants enregistrés pour transférer l'argent depuis les comptes PayPal.

Les pirates parviennent à créer des e-mails d'hameçonnage très sophistiqués notamment grâce à la collecte d'informations personnelles publiques disponibles sur le web – accessibles sur les réseaux sociaux par exemple. Il est alors essentiel pour l'utilisateur de poster le moins d'informations possibles sur Internet ou de s'assurer que celles-ci sont en mode privé. Il est également crucial de supprimer ses comptes s'ils ne sont plus utilisés, car bien qu'abandonnés, ces profils restent en ligne et des personnes malintentionnées pourraient usurper l'identité de l'internaute ou nuire à sa réputation en ligne en utilisant des informations sensibles contre lui.
La protection de la vie privée et des données personnelles (vol de ses données personnelles) implique une modification du comportement des internautes à commencer par de meilleures méthodes de gestion de mots de passe, une vigilance accrue sur leur utilisation d'Internet et des informations personnelles partagées publiquement – comme sur les réseaux sociaux. Au-delà des bonnes pratiques, il existe des solutions qui répondent aux problématiques liées à la vie privée. Cependant face aux menaces, il n'appartient qu'à nous de nous discipliner et de tout mettre en œuvre pour protéger nos données personnelles.

Article original de Damien Bancal

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

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

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Devenir maître dans l'art de protéger sa vie privée sur le net – Data Security BreachData Security Breach

Attention ! Le Cloud est espionné

	Attention ! Le Cloud est espionné

Les agences gouvernementales peuvent exploiter la 'fonctionnalité' d'écoute des hyperviseurs pour récupérer des données depuis le cloud. Si vous n'êtes pas propriétaire du hardware, vous n'êtes pas propriétaire des données, selon une étude de Bitdefender.

L'éditeur de solutions de sécurité informatique affirme que les agences gouvernementales peuvent exploiter la 'fonctionnalité' d'écoute des hyperviseurs pour récupérer des données depuis le cloud. Les révélations de l'affaire Snowden sur les capacités d'interception des données de la part de la NSA et de ses agences partenaires ont incité les propriétaires d'infrastructures et les fournisseurs de services, ainsi que les utilisateurs, à s'assurer que leurs données sont échangées sans encourir de risque de confidentialité et qu'elles sont stockées sous forme chiffrée. Régulièrement, les chercheurs s'attaquent à des protocoles très utilisés ou à leur mode de mise en œuvre. Des failles sont ainsi découvertes de manière récurrente et corrigées à plus ou moins brèves échéances, comme dans le cas de vulnérabilités bien connues telles que Heartbleed ou Logjam, qui ont entraîné le déploiement massif de correctifs à une échelle jusque-là inédite.
Mais les entreprises, et par conséquent, leurs clients, sont-elles vraiment protégées une fois que ces failles sont corrigées ? Existe-t-il des méthodes dissimulées et plus ou moins légales que les organismes d'État et certaines grandes entreprises bien informées seraient susceptibles d'utiliser pour passer outre les protocoles TLS / SSL, censés protéger les échanges d'informations ? Bref, espionnage dans le Cloud possible ?
Le 26 mai 2016, lors de la Conférence HITB à Amsterdam, Radu Caragea, Chercheur en sécurité des Bitdefender Labs, a démontré lors d'un POC (preuve de concept), que la communication protégée peut être déchiffrée en temps réel, en utilisant une technique qui ne laisse pratiquement aucune empreinte et qui reste invisible pour presque tout le monde, sauf peut-être pour des auditeurs de sécurité particulièrement vigilants.

Espionnage dans le cloud : Quelles conséquences pour votre sécurité ?
Cette attaque permet à un fournisseur de services cloud mal intentionné (ou sur lequel on a fait pression pour qu'il donne des accès à des agences gouvernementales) de récupérer les clés TLS utilisées pour chiffrer chaque session de communication entre votre serveur virtualisé et vos clients (même si vous utilisez Perfect Forward Secrecy !). Si vous êtes un DSI et que votre entreprise externalise son infrastructure de virtualisation auprès d'un prestataire de service, considérez que toutes les informations circulant entre vous et vos utilisateurs ont pu être déchiffrées et lues pendant une durée indéterminée.
Il est impossible de savoir dans quelle mesure vos communications ont pu être compromises et pendant combien de temps, puisque cette technique ne laisse aucune trace anormale derrière elle. Les banques et les entreprises qui gèrent des dossiers de propriété intellectuelle ou des informations personnelles, ainsi que les institutions gouvernementales sont les secteurs susceptibles d'être particulièrement touchés par cette faille.

Espionnage dans le Cloud : Premières découvertes
Cette nouvelle technique, surnommée TeLeScope, a été développée par l'éditeur dans le cadre de ses recherches et permet à un tiers d'écouter les communications chiffrées avec le protocole TLS, entre l'utilisateur final et une instance virtualisée d'un serveur. Cette technique n'est opérationnelle qu'avec les environnements virtualisés fonctionnant au-dessus de l'hyperviseur. Ces infrastructures sont extrêmement répandues et sont proposées par les géants de l'industrie tels qu'Amazon, Google, Microsoft ou DigitalOcean, pour ne citer qu'eux. Si la plupart des experts de l'industrie s'accordent pour dire que la virtualisation est l'avenir, aussi bien en termes de stockage, que de déplacement et de traitement de gros volumes de données, ce type de solutions fait déjà partie du quotidien de nombreuses entreprises.
Plutôt que d'exploiter une faille dans le protocole TLS, cette nouvelle technique d'attaque repose sur l'extraction des clés TLS au niveau de l'hyperviseur par une inspection intelligente de la mémoire. Même si l'accès aux ressources virtuelles de la VM est une pratique déjà connue (accéder au disque dur de la machine, par exemple), le déchiffrement en temps réel du trafic TLS, sans mettre en pause la machine virtuelle de manière flagrante et visible, n'avait jamais été réalisé jusqu'alors.
La découverte de ce vecteur d'attaque a été possible en recherchant un moyen de surveiller des activités malveillantes depuis le réseau de honeypots de l'éditeur, sans altérer la machine et sans que les pirates puissent comprendre qu'ils sont surveillés. Un administrateur réseau ayant accès à l'hyperviseur d'un serveur hôte pourrait surveiller, exfiltrer et monétiser toutes les informations circulant depuis et vers le client : adresses e-mail, transactions bancaires, conversations, documents professionnels confidentiels, photos personnelles et autres données privées.

Espionnage dans le Cloud : Comment cela fonctionne-t-il ?
Normalement, la récupération des clés à partir de la mémoire d'une machine virtuelle nécessiterait de mettre en pause la VM et de décharger le contenu de sa mémoire sur un fichier. Ces deux processus sont intrusifs et visibles par le propriétaire de la VM (de plus ils enfreignent le SLA – Service Level Agreement). L'approche des chercheurs repose sur les mécanismes de Live Migration, disponibles au sein des hyperviseurs modernes, qui nous permettent de réduire le nombre de pages nécessaire pour le vidage de la mémoire de l'ensemble de la RAM, à celles modifiées lors de l'établissement d'une liaison TLS.
« ***Au lieu de mettre la machine en pause (ce qui entrainerait une latence notable) et de réaliser un vidage complet de la mémoire, nous avons développé une technique de différentiel de la mémoire qui utilise des fonctions de base déjà présentes dans les technologies de l'hyperviseur,*** » explique Radu Caragea. « ***Ensuite, bien que cela permette de réduire le volume de vidage mémoire de giga-octets à méga-octets, le temps nécessaire pour écrire une telle quantité de données sur un espace de stockage reste non négligeable (de l'ordre de quelques millisecondes) et c'est pourquoi nous montrons comment 'déguiser ' le processus pour le faire passer pour une latence du réseau, sans qu'il soit nécessaire de stopper la machine.*** »

Atténuation des risques
L'attaque TeLeScope n'exploite pas de faille lors de l'implémentation du protocole TLS et ne tente pas de contourner le niveau de chiffrement de l'implémentation TLS via des attaques par repli (downgrade attacks). Au lieu de cela, elle exploite une caractéristique de l'hyperviseur pour exfiltrer les clés utilisées par le protocole pour chiffrer la session. Notre POC révèle un écart fondamental qui ne peut être corrigé ou atténué sans réécrire les bibliothèques de cryptographie qui sont déjà en cours d'utilisation. La seule solution à ce jour est, en premier lieu, de bloquer l'accès à l'hyperviseur – en exécutant votre propre hardware à l'intérieur de votre propre infrastructure.
Article original de Damien BANCAL

Denis JACOPINE est Expert informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

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

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : ZATAZ Espionnage dans le Cloud – ZATAZ

Cloud et sécurité : le point sur 7 questions qui fâchent

Cloud et sécurité : le point sur 7 questions qui fâchent

Le nuage informatique est à la mode chez les grands comptes, mais aussi chez les PME et TPE qui n'hésitent plus, parfois, à y déverser des données sensibles. La prudence reste pourtant de mise.

En France, le marché du "cloud" n'est pas encore mature », confie Henry-Michel Rozenblum, délégué général d'EuroCloud France, l'association des fournisseurs français de « cloud » liée à la fédération européenne Eurocloud. Ce qui signifie qu'il n'y a pas de standard de sécurité spécifique. L'approche consiste plutôt à s'appuyer sur les bonnes pratiques traditionnelles de la sécurité informatique. Notamment la certification ISO 27001, qui, si elle est délivrée par un grand cabinet d'audit, est la seule garantie qui fait foi. Autrement, pas de véritable sécurité. *« Même si le discours marketing prétend le contraire »,* souligne Gérôme Billois, expert sécurité au Cercle européen de la sécurité et des systèmes d'information.

Les pirates s'adaptent

Il existe sur Internet, des « black markets » électroniques (places de marché pirates), où des logiciels clefs en main s'échangent sans contrôle. Ils permettent de mener des attaques complexes contre un « cloud », sans même avoir besoin de solides compétences en informatique. Leur nom : des « hyperkits ». *« En quelques clics, ils permettent de prendre le contrôle d'un serveur physique à partir du serveur virtuel »,* prévient Jean-Paul Smets, PDG de Vifib, un offreur de « cloud » distribué. *« L'unique manière de s'en protéger est de maintenir son système à jour et de combler systématiquement les failles de sécurité. »*

Un risque systémique

En dehors des attaques, rappelons que le **cloud est, lui-aussi, sensible aux bugs, pannes et erreurs humaines…** *« Comme une poignée d'opérateurs de "cloud" domine le marché, le moindre problème prend une ampleur démesurée »,* explique Gabriel Chadeau, directeur commercial chez Vision Solutions, spécialiste de la récupération de données. Normal : lorsque le nuage « plante », des milliers d'entreprises n'accèdent plus à leurs services. Pour se protéger, il faut se demander quels services externaliser dans le « cloud » et quels autres garder chez soi. *« Je déconseille de mettre ses applications métiers dans le cloud. Pour des raisons de disponibilité et de confidentialité »,* souligne Gérôme Billois.

Une confidentialité illusoire

Pour de nombreux acteurs, la **confidentialité est le point noir du cloud computing**. Les fournisseurs américains sont particulièrement visés par les critiques. Car le **Patriot Act les oblige ainsi que leurs filiales situées en dehors des Etats-Unis à remonter des données vers leurs autorités**. En novembre 2012, le rapport « cloud computing » dans l'enseignement supérieur et les instituts de recherche et le Patriot Act américain, rédigé par des juristes de l'université d'Amsterdam, expliquait qu'il s'agissait d'un droit *« extraterritorial »* et qu'il ne s'embarrasse pas des lois nationales ou européennes… En ce moment, l'Europe légifère sur le sujet. En attendant, mieux vaut se rabattre sur un offreur cloud français.

De l'espionnage en interne

Reste qu'un fournisseur français n'est pas un gage de sécurité en soi. *« Parce que, lorsqu'une donnée circule dans le nuage, des centaines de techniciens y ont accès. Par le jeu de la sous-traitance, plus de la moitié d'entre eux ne sont pas en France »,* assure Hervé Schauer, membre du Club de la sécurité de l'information français (Clusif) et expert en sécurité des systèmes d'information. *« Si l'une de ces personnes est corrompue, il n'y a plus de confidentialité dans le cloud. »* Pour se prémunir, il faut obliger son fournisseur à apporter des garanties concrètes. *« Il doit pouvoir expliquer comment son architecture est techniquement cloisonnée et comment les droits sont gérés »,* explique Matthieu Bennasar, consultant sécurité au Lexsi, un cabinet spécialisé en sécurité informatique et gestion des risques.

Chiffrement faible

A défaut d'obtenir ces garanties, il faut vivre avec la crainte d'être mis sur écoute, dans le nuage. Et le bon vieil argument qui veut que le chiffrement protège efficacement les données contre les regards malveillants ne tient en réalité pas la route. C'est un écran de fumée. *« Aucun chiffrement n'est infaillible »,* rappelle Patrick Debus-Pesquet, directeur technique chez Numergy, un des deux opérateurs de cloud souverain. Ce qu'il faut faire, souvent, c'est auditer son cloud afin de déceler la présence de sondes et de logiciels espions.

Pas d'audit par défaut

Mais encore faut-il pouvoir auditer son cloud ! Tous les offreurs ne le permettent pas. *« Il faut négocier en amont une clause d'auditabilité, c'est indispensable »,* martèle Philippe Hervias, directeur sécurité à l'Institut français de l'audit et du contrôle interne (Ifaci).

Réversibilité impossible

Dans tous les cas, négocier avec son fournisseur est une stratégie gagnante. Dans le cas inverse, le risque est de se retrouver piégé avec un mauvais prestataire. Et de ne pas pouvoir en changer, parce qu'il est difficile – voire impossible – de réinjecter ses données dans un nouveau système d'information. *« Je n'ai jamais vu un tel principe mis en œuvre »,* admet Pierre-Josée Billotte, président du conseil d'administration d'Eurocloud France. Il faut donc redoubler de vigilance au moment de signer son contrat. Ou choisir exclusivement des applications SaaS à base de logiciels libres que l'on peut répliquer gratuitement sur une autre plate-forme.

Article original de GUILLAUME PIERRE

Réagissez à cet article

Original de l’article mis en page : Cloud et sécurité : le point sur 7 questions qui fâchent – Les Echos Business