Combien vous coûterait le piratage de vos données ?

Combien vous coûterait le piratage de vos données ?

Un consommateur français sur trois reconnaît que sa loyauté envers une marque diminue après qu'une attaque informatique a porté atteinte aux données qu'il lui avait confié.

Souvent préparées de longues dates, les attaques informatiques qui frappent les entreprises laissent des traces longtemps après.
Publiée aujourd'hui, une étude internationale menée par Vanson Bourne, pour l'éditeur de logiciels de cybersécurité FireEye, souligne que les conséquences de tels épisodes entament la performance commerciale de la société victime, au-delà des dégâts informatiques des premiers jours. « *La sécurité des systèmes d'information a un réel impact sur la confiance des consommateurs* », affirme Yogi Chandiramani, directeur des ventes en Europe pour FireEye.
« *En France, l'attaque qui a touché TV5 Monde en avril 2015 et les vols de données chez Orange en 2014 ont particulièrement marqué les esprits* », poursuit-il. 34 % des consommateurs français reconnaissent que leur loyauté en tant que client actuel ou potentiel d'une marque diminue après qu'une entreprise a laissé fuiter des données, pointe le questionnaire en ligne envoyé à 1.000 d'entre eux. Un argument de plus pour ceux qui voient les efforts de cyber-sécurité comme un argument de compétitivité .
L'atteinte à leurs données personnelles refroidit particulièrement les ardeurs à l'achat des consommateurs. Quand le vol de données est connu, plus de trois Français sur quatre déclarent qu'ils stopperaient leurs emplettes de produits ou services fournis par la victime, surtout si la faute vient de l'équipe dirigeante – ils sont plus conciliants s'il s'agit de l'erreur humaine d'un subordonné. La tendance se confirme au fil des années. D'après l'étude, 61 % des Français déclarent avoir pris en considération la sécurité de leurs données lors de leurs achats en 2015. Ils n'étaient que 53% dans cet état d'esprit en 2014…

Après une cyber-attaque, la transparence prime

A cette perte de chiffre d'affaires potentiel s'ajoute le risque de poursuite en justice. La moitié des Français déclarent qu'ils engageraient des poursuites contre l'entreprise cyber-attaquée qui n'a pas su protéger leurs données personnelles, volées ou utilisées à des fins criminelles. Aux Etats-Unis, Target et Sony Picture s ont été attaqués en Justice par des procédures de class action, le premier par ses clients, le second par ses salariés.
Dès lors, la tentation peut être grande pour une entreprise de garder secret le fait que son système d'information ait été vulnérable à des cyber-criminels. Ce serait pourtant aggraver le mal qui surviendra au moment où, inévitablement à l'heure d'Internet, l'information ressortira.
« *Les consommateurs pointent les négligences des entreprises mais attendent surtout d'elles de la transparence, 93 % d'entre eux souhaitent être prévenus dans les 24h quand leurs données sont exposées* », prévient Yogi Chandiramani.

Des changements dans quelques mois ?

Le règlement européen sur la protection des données, qui devrait s'appliquer en France d'ici 2018, prévoit d'imposer aux sociétés de notifier les autorités, voir leurs clients, de toutes atteintes sur les données personnelles des citoyens européens dans les 72h après la découverte du problème.
A noter :
L'attaque particulièrement destructrice qui a touché TV5Monde en 2015 devrait coûter près de 10 millions d'euros sur trois ans, uniquement en réparation informatique… [Lire la suite]

Réagissez à cet article

Source : *Cyber-attaque : les coûts d'après, Cybersécurité – Les Echos Business*

La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

Aux États-Unis, une affaire judiciaire pose la question du droit que peuvent avoir les autorités judiciaires à contraindre un suspect à débloquer son iPhone avec le capteur Touch ID qui permet d'accéder au contenu du téléphone avec les empreintes digitales.

La question s'est certainement déjà posée dans les commissariats et dans les bureaux des juges d'instruction, et elle devrait devenir plus pressant encore dans les années à venir : alors qu'un suspect peut toujours prétendre avoir oublié son mot de passe, ou refuser de répondre, les enquêteurs peuvent-ils contraindre un individu à débloquer son téléphone lorsque celui-ci est déblocable avec une simple empreinte digitale ?
Le débat sera tranché aux États-Unis par un tribunal de Los Angeles. Le Los Angeles Times rapporte en effet qu'un juge a délivré un mandat de perquisition à des policiers, qui leur donne le pouvoir de contraindre physiquement la petite amie d'un membre d'un gang arménien à mettre son doigt sur le capteur Touch ID de son iPhone, pour en débloquer le contenu.

Le mandat signé 45 minutes après son placement en détention provisoire a été mis en œuvre dans les heures qui ont suivi. Le temps était très court, peut-être en raison de l'urgence du dossier lui-même, mais aussi car l'iPhone dispose d'une sécurité qui fait qu'au bout de 48 heures sans être débloqué, il n'est plus possible d'utiliser l'empreinte digitale pour accéder aux données. Mais l'admissibilité des preuves ainsi collectées reste sujette à caution et fait l'objet d'un débat entre juristes.

EN MONTRANT QUE VOUS AVEZ OUVERT LE TÉLÉPHONE, VOUS DÉMONTREZ QUE VOUS AVEZ CONTRÔLE SUR LUI
Certains considèrent qu'obliger un individu à placer son doigt sur le capteur d'empreintes digitales de son iPhone pour y gagner l'accès revient à forcer cette personne à fournir elle-même les éléments de sa propre incrimination, ce qui est contraire à la Constitution américaine et aux traités internationaux de protection des droits de l'homme. « En montrant que vous avez ouvert le téléphone, vous montrez que vous avez contrôle sur lui », estime ainsi Susan Brenner, une professeur de droit de l'Université de Dayton. Le capteur Touch ID ne sert pas uniquement à débloquer le téléphone, mais aussi à le déchiffrer, en fournissant une clé qui joue le rôle d'authentifiant du contenu.
D'autres estiment qu'il s'agit ni plus ou moins que la même chose qu'une perquisition à domicile réalisée en utilisant la clé portée sur lui par le suspect, ce qui est chose courante et ne fait pas l'objet de protestations. Ils n'y voient pas non plus de violation du droit de garder le silence, puisque le suspect ne parle pas en ne faisant que poser son doigt sur un capteur.

ET EN FRANCE ?
Pour le moment, le sujet n'est pas venu sur la scène législative en France. Mais il pourrait y venir par analogie avec d'autres techniques d'identification biométrique.
En matière de recherche d'empreintes digitales ou de prélèvement de cheveux pour comparaison, l'article 55-1 du code de procédure pénale punit d'un an de prison et 15 000 euros d'amende « le refus, par une personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre une infraction, de se soumettre aux opérations de prélèvement ». De même en matière de prélèvements ADN, le code de procédure pénale autorise les policiers à exiger qu'un prélèvement biologique soit effectué sur un suspect, et « le fait de refuser de se soumettre au prélèvement biologique est puni d'un an d'emprisonnement et 30 000 euros d'amende ».
Sans loi spécifique, les policiers peuvent aussi tenter de se reposer sur les dispositions anti-chiffrement du code pénal, puisque l'empreinte digitale sert de clé. L'article 434-15-2 du code pénal punit de 3 ans de prison et 45 000 euros d'amende le fait, « pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités ». Mais à notre connaissance, elle n'a jamais été appliquée pour forcer un suspect à fournir lui-même ses clés de chiffrement, ce qui serait potentiellement contraire aux conventions de protection des droits de l'homme… [Lire la suite]

Réagissez à cet article

Source : *La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ? – Politique – Numerama*

Airbus déjoue douze attaques informatiques majeures par an

Airbus déjoue douze attaques informatiques majeures par an

Source : *Piratage informatique : Airbus déjoue douze attaques majeures par an – 06/05/2016 – ladepeche.fr*

article de Gil Bousquet

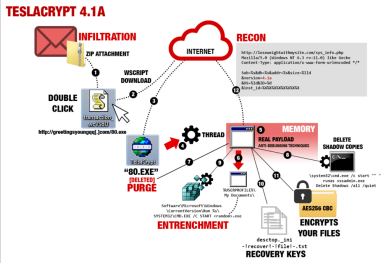
Le CryptoVirus TeslaCrypt s’attaque à de nouveaux fichiers et améliore sa protection

Le CryptoVirus TeslaCrypt s’attaque à de nouveaux fichiers et améliore sa protection

---

Ces nouveaux exemplaires de TeslaCrypt sont diffusés massivement en tant que pièce jointe dans des spams qui imitent les avis de réception de colis des courriers express. D'après Endgame, la version 4.1A est apparue il y a environ une semaine ; outre les extensions déjà ciblées, elle attaque également les fichiers suivants .7z, .apk, .asset, .avi, .bak, .bik, .bsa, .csv, .d3dbsp, .das, .forge, .iwi, .lbf, .litemod, .litesql, .ltx, .m4a, .mp4, .rar, .re4, .sav, .slm, .sql,

La diffusion de TeslaCryp via le spam constitue également un changement : lors des campagnes récentes de TeslaCrypt, le ransomware avait été propagé via des kits d'exploitation et des redirections depuis des sites WordPress et Joomla. Dans ce cas, la victime doit ouvrir le fichier ZIP en pièce jointe afin d'activer un downloader JavaScript qui utilise Wscript (un composant de Windows) pour télécharger le fichier binaire de TeslaCrypt depuis le domaine greetingsyoungqq[.]com.
D'après notre interlocutrice, l'analyse de la version actualisée du ransomware fut complexe car elle lance de nombreux flux d'application et d'opérations de débogage afin de compliquer la tâche des outils de protection. Comme l'explique Amanda Rousseau, « il semblerait qu'il essaie de dissimuler les lignes dans la mémoire. Il est plus difficile pour l'Antivirus de les détecter s'il n'analyse pas la mémoire. »



Le recours à Wscript rend également la détection plus compliquée car le trafic ressemble à des communications légitimes de Windows. Selon Amanda Rousseau, il aura fallu quatre jours aux outils de détection pour identifier la technique et l'ajouter aux signatures. La durée de service des serveurs de commande sur lesquels se trouve TeslaCrypt a été limitée. A l'issue de celle-ci, les individus malintentionnés changent d'hébergement.
La version actualisée du ransomware utilise également un objet COM pour dissimuler les lignes de code extraites et élimine les identifiants de zone afin qu'ils ne soient pas découverts. De plus, pour éviter la surveillance, le malware arrête plusieurs processus Windows : Task Manager, Registry Editor, SysInternals Process Explorer, System Configuration et Command Shell. Pour garantir sa présence permanente, il se copie sur le disque et crée le paramètre correspondant dans la base de registres.
Vous trouverez une description technique détaillée de TeslaCrypt, y compris de ses méthodes de chiffrement et de ses techniques de lutte contre le débogage sur le blog d'Endgame.
Amanda Rousseau a indiqué dans ses commentaires que lors des essais, les nouveaux échantillons ont atteint les disques réseau connectés et ont tenté de chiffrer les fichiers qui s'y trouvaient. Ils tentent également de supprimer le cliché instantané du volume afin de priver la victime de toute chance de récupération.
Mais il y a malgré tout une bonne nouvelle : la version actualisée de TeslaCrypt chiffre les fichiers à l'aide d'une clé AES 256 et non pas à l'aide d'une clé RSA de 4 096 bits comme indiqué dans la demande de rançon et qui plus est, les informations indispensables au déchiffrement restent sur la machine infectée. « Nous avons trouvé l'algorithme de chiffrement : il fonctionne correctement, mais laisse le fichier de restauration dans le système » a confirmé Amanda Rousseau. « Si l'on part du programme de déchiffrement antérieur de TeslaCrypt et que son code est actualisé conformément aux [découvertes], il sera possible de réaliser le déchiffrement. » Il y a un an environ, Cisco a diffusé un utilitaire de ligne de commande capable de déchiffrer les fichiers touchés par TeslaCrypt.
Amanda Rousseau a également signalé que les auteurs de la version actualisée du ransomware avait emprunté beaucoup de code aux versions antérieures, notamment l'utilisation des objets COM et certaines techniques de débogage. « On dirait que les individus malintentionnés suivent les chercheurs à la trace en surveillant le code [de déchiffrement] publié sur Github en open source » explique le président d'Endgame en montrant les modifications introduites au cours du dernier mois depuis la version 4.0 jusqu'à la version 4 1A. – De petites modifications sont introduites dans chaque version et à la sortie de chaque nouveau décrypteur. Il prenne le meilleur de ce qui était utilisé il y a deux mois et l'appliquent aujourd'hui. »… [Lire la suite]

Source : *TeslaCrypt s'attaque à de nouveaux fichiers et améliore sa protection – Securelist*

Une alerte à la bombe dans un avion causée par un réseau Wi-Fi

Une alerte à la bombe dans un avion causée par un réseau Wi-Fi

Les passagers d'un vol interne australien ont eu une petite frayeur à cause d'un réseau WiFi.

Le réseau WiFi en question a été repéré par un des passagers qui, inquiet de ce nom étrange, en a tout de suite informé le personnel de bord. Ce dernier a alors remonté l'information jusqu'au commandant de bord, qui a décidé de garder l'avion au sol tant que l'appareil émetteur de ce réseau n'a pas été repéré. Une annonce retentit dans les hauts parleurs de l'avion afin de prévenir les passagers, mais après une demi-heure de recherche, la source n'est toujours pas localisée.
« Un réseau WiFi peut avoir une bonne portée, donc cela aurait pu venir d'une personne dans le terminal », explique un des passagers. Des recherches sont menées dans et autour de l'avion, sans résultat. Finalement, après trois heures d'attente sur le tarmac, l'avion se met finalement en route pour sa destination, Perth, en Australie, où il atterrit sans encombre 80 minutes plus tard... [Lire la suite]

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

- Expertises techniques (virus, espions, piratages, arnaques Internet...) et judiciaires (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

Suivez-nous sur

Réagissez à cet article

Source : *Une alerte à la bombe dans un avion causée par un réseau Wi-Fi*

Forum TAC « Technologies Against Crime » : LYON, les 28 et 29 avril 2016

Forum TAC « Technologies Against Crime » : LYON, les 28 et 29 avril 2016

Forum TAC « Technologies Against Crime » est un Forum destiné à rassembler les meilleurs spécialistes internationaux dans la lutte contre la Cybercriminalité. Il a lieu cette année au Centre des Congrès de LYON, les 28 et 29 avril 2016.

Cette année, le thème est :

Les révolutions technologiques : réponses aux nouvelles formes de la criminalité ?

TECHNOLOGY AGAINST CRIME
INTERNATIONAL FORUM ON TECHNOLOGIES FOR A SAFER WORLD
APRIL 28 & 29 2016
CENTRE DE CONGRÈS LYON-FRANCE

Sous le haut patronage de — Avec le soutien de — Un événement co-organisé par

Les principaux partenaires de l'événement

Tout au long de ces 2 jours, nous allons assister aux présentation des sujets suivants :

• Cyber sécurité, apport de la technologie à la sécurité sur le net.
• Gestion de l'identité : la demande mondiale (pays développés et pays émergents), les évolutions technologiques, la lutte contre les fraudes à l'identité.
• Les nouvelles formes du terrorisme, l'apport de la technologie à la prévention, à la détection et au suivi.
• Défense des libertés et de la vie privée : comment tenir compte de ces exigences dès la conception du produit, « Privacy by design ».
• Les progrès de la technologie pour détecter les nouvelles contrefaçons (médicaments, matériel électronique, métaux…).
• Gestion des catastrophes et des grands événements, protection civile.
• Protection des infrastructures et des ressources critiques.
• Sécurité des villes connectées.
• Les progrès techniques au service de l'enquête judiciaire.
• Big Data : risques et opportunités dans le domaine de la sécurité.

Réagissez à cet article

Source : *FITS – Présentation*

Quels sont les dangers des points d’accès Wifi gratuits ?

	**Quels sont les dangers des points d’accès Wifi gratuits ?**

Selon une étude mondiale d'iPass, 62% des entreprises interdisent à leurs employés mobiles d'utiliser les points d'accès Wi-Fi gratuits considérés comme des menaces.

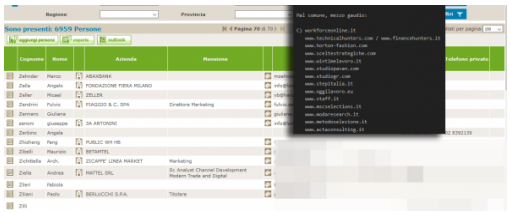
De plus en plus nombreux, les points d'accès Wi-Fi ouverts et gratuits (dans les rues, les parcs, les gares…) sont bien pratiques pour se connecter en mobilité, notamment pour les salariés nomades. Mais ces hotspots ne brillent pas toujours par leur sécurité. D'ailleurs, les entreprises s'inquiètent de plus en plus des risques liés à leur utilisation par leurs employés. La possibilité de voir des données sensibles détournées est forte, du coup, de plus en plus d'entreprises optent pour une solution radicale : interdire leur usage.
C'est la conclusion d'une étude iPass (un spécialiste des accès Wi-Fi pour les pros) menée par Vanson Bourne au mois de mars 2016 auprès de 500 directeurs informatiques et décideurs informatiques aux États-Unis (200), au Royaume-Uni (100), en Allemagne (100) et en France (100).
Ainsi, près des deux tiers (62%) des entreprises interdisent à leurs employés mobiles d'utiliser les points d'accès Wi-Fi gratuits, 20% ont déclaré qu'elles envisageaient d'interdire cet accès dans un avenir proche et 94% des entreprises interrogées considèrent les points d'accès Wi-Fi gratuits comme une source importante de menaces pour la sécurité mobile.
En France, 29% des directions interrogées interdisent systématiquement cet accès, 44% parfois, soit un total de 73%. Et 17% pensent le faire dans le futur. Les interdictions concernent avant tout le secteur de la finances où l'interdiction totale et temporaire atteint 85%, devant l'IT (80%).

VPN

« La méthode consistant à leur empêcher tout accès à ces points de connectivité est aussi maladroite qu'inadaptée. Dans le monde actuel, où le Wi-Fi occupe la première place, les entreprises doivent impérativement informer leurs employés mobiles des dangers du Wi-Fi gratuit et non sécurisé, et leur donner les outils adéquats pour sécuriser leur connexion à Internet et rester productifs. », souligne iPass qui rappelons-le fournit des solutions de sécurisation dédiées…
« Le Wi-Fi est une technologie révolutionnaire qui a bouleversé le mode de travail des utilisateurs dans le monde », explique Keith Waldorf, Vice-président du département d'ingénierie chez iPass. « Cependant, elle est à l'origine de problèmes colossaux en termes de sécurité mobile. Le fait de rester connecté est un besoin de base pour tout employé mobile. Toutefois, comme le nombre d'entreprises victimes d'atteintes à la sécurité ne cesse de croître, la question de la sécurité mobile devient un sujet brûlant pour un grand nombre de sociétés. En particulier, le recours à des points d'accès Wi-Fi gratuits, non sécurisés, inquiète de plus en plus les entreprises, qui essaient de trouver un équilibre entre les coûts et la convivialité d'une solution de connectivité et les menaces éventuelles des pirates informatiques ».
Pour 37% des participants interrogés, les points d'accès Wi-Fi gratuits représentent la plus grande menace à gérer en termes de sécurité mobile, d'abord à cause du manque de précautions prises par les employés (36%) et pour 27%, des appareils qu'ils utilisent. Du coup, 88% des entreprises (94% en France) ont beaucoup de difficultés à appliquer à une stratégie standardisée.
Pour autant, des solutions simples existent : d'abord la pédagogie auprès des salariés nomades puis la technique avec la mise en place d'un VPN (Virtual Private Technology), qui crée une connexion chiffrée. Toutefois, seuls 26 % des participants à l'étude sont certains que ses employés utilisent uniquement les réseaux VPN pour accéder aux systèmes professionnels… [Lire la suite]

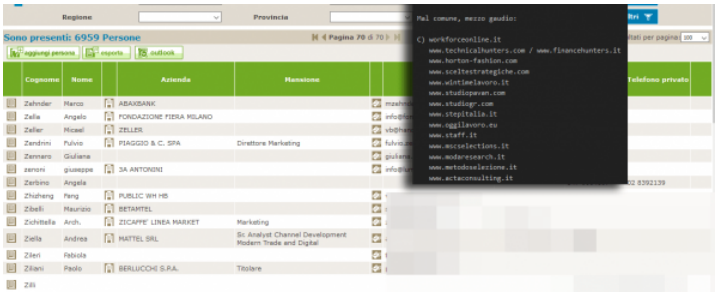
Source : *Wi-Fi : les points d'accès gratuits donnent des sueurs froides aux entreprises – ZDNet*

Des milliers de données clients diffusées sur Internet par Anonymous



Des milliers de données clients diffusées sur Internet par Anonymous

Données clients diffusées sur Internet – Des internautes ont lancé, sous la signature Anonymous, une opération contre le business des laboratoires pharmaceutiques. Ils veulent dénoncer « les porcs et les connivences entre les gouvernements et les sociétés« . En Italie, c'est un hébergeur qui fait les frais d'une cyber action.



Étonnante revendication que celle lancée par les Anonymous. Lundi 11 avril, des internautes ont lancé un appel pour cibler « ***les porcs et les connivences entre les gouvernements et les sociétés pharmaceutiques***« . Pour les organisateurs, la mission est de collecter des informations, des données, pour les diffuser ensuite. « ***Nous voulons dire la vérité sur le cancer, la nutrition, les médicaments…*** » indique les personnes cachées derrière la signature et le masque Anonymous. « ***Notre santé est plus importante que leur profit !*** […] ***Beaucoup d'entre vous ont déjà pris conscience de ce système axé sur les profits, il est temps de prendre des mesures, il est temps d'exposer la corruption et demande justice pour les victimes*** ».

En Italie, des données clients diffusées sur Internet

En Italie, l'agence web Engitel, basée à Milan, se faisait pirater et voler plusieurs milliers de données par Anonymous Italia et un second groupe du nom de LulzSecITA. 40 sites impactés, plus de 2 800 fichiers sensibles ont d'abord été diffusés. Ici pas d'attaque SQL, mais ce qui semble être une copie conforme des données clients, et leur site web, via l'espace d'administration de l'entreprise Milanaise.

Anonymous Italie, la source initiale de la fuite, a affirmé qu'il y avait plus de 1,8 millions de données d'utilisateurs. Ils vont le prouver en diffusant plusieurs autres dossiers, via MEGA. Dans l'un des dossier que j'ai pu consulter, des fichiers qui permettent de contacter les responsables des sites Internet (J'ai pu en dénombre 6 959) de sociétés italiennes telles que MTV Italie, La Repubblica, Facebook Italie, Gucci, FastWeb, Microsoft, Wind, Ducati… « ***Voici notre premier chapitre de notre opération Nessun Dorma,*** indique les hacktivistes. ***Nous sommes fatigués des mensonges habituels diffusés dans tous les médias au sujet du monde du travail*** ».

Bref, comme l'indiquent les pirates dans leur – communiqué de presse – : Si vous voulez la paix, préparez la guerre. A noter que plusieurs sites Suisses (aiti.ch, e-lavoro.ch, aitiservizi.ch, e-impresa.ch, jobopportunity.ch, BFKconsulting.ch, helvia.ch et workandwork.ch) ont été piratés lors de cette opération… [Lire la suite]

Réagissez à cet article

Source : *ZATAZ Anonymous : des milliers de données clients diffusées sur Internet – ZATAZ*

Apple a essayé d'aider le père de l'enfant mort à récupérer des données

Apple a essayé d'aider le père de l'enfant mort à récupérer des données

---

Contrairement à ce que disent officiellement ses conditions d'utilisation, Apple accepte bien, au cas par cas, de donner à des vivants l'accès aux données iCloud d'un utilisateur mort.
Il y a ce qu'Apple écrit dans ses conditions d'utilisation, et il y a la pratique, plus humaine. À la suite de la lettre envoyée à Tim Cook par ce père endeuillé, qui souhaitait avoir accès aux données de l'iPhone de son enfant de 13 ans mort d'un cancer des os, CNN rapporte qu'Apple a bien essayé de venir en aide à l'architecte italien Leonardo Fabbretti.

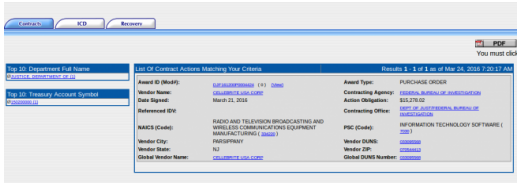
Fidèle à sa position de principe, Apple n'a pas accepté de tenter de casser la protection de l'iPhone 6 de l'enfant, qui aurait permis d'accéder aux données chiffrées contenues sur le téléphone, y compris aux photos et vidéos prises par l'enfant peu avant sa mort.
En revanche, au terme de quelques conversations, les équipes d'Apple ont bien accepté de regarder si des données n'avaient pas été synchronisées avec un cloud iCloud, ce qui aurait permis de les divulguer au père – il n'y avait toutefois aucune sauvegarde.

CE N'EST PAS LE PREMIER ÉCART QU'APPLE ACCEPTE DE RÉALISER, SANS JAMAIS ACCEPTER D'EN FAIRE UNE POLITIQUE GÉNÉRALE
Officiellement, Apple (qui a refusé de commenter) ne réalise pourtant pas ce type d'opération, y compris au bénéfice des parents ou des héritiers d'un défunt. « Dès réception d'une copie d'un certificat de décès, votre Compte pourra être résilié et l'intégralité du Contenu de votre Compte pourra être supprimée », dit simplement le contrat des conditions d'utilisation d'iCloud.
Il indique que le compte iCloud est « incessible et que tous les droits liés à votre identifiant Apple ou Contenu dans le cadre de votre Compte seront résiliés au moment de votre décès ».

Ce n'est pas le premier écart qu'Apple accepte de réaliser, sans jamais accepter d'en faire une politique générale, ni même de reconnaître officiellement des critères d'exceptions. Début 2016, au Canada, une veuve avait déjà obtenu d'Apple qu'il lui transmette les données de son défunt mari. Mais le transfert n'avait pu être obtenu qu'après médiatisation de l'affaire, et intervention d'une association.
L'article de CNN rapporte par ailleurs que Leonardo Fabbretti a pu rencontrer les équipes de l'entreprise israélienne Cellebrite qui propose de l'aider gratuitement à accéder aux données de l'iPhone 6.
Pour le moment, les hackers employés par le FBI pour débloquer l'iPhone 5C du tueur de San Bernardino auraient réussi à extraire le listing des données stockées, mais pas encore les données elles-mêmes. Ils se diraient toutefois « optimistes » sur leurs chances de succès. S'ils parvenaient à débloquer ainsi un iPhone 6, réputé plus sûr, l'annonce viendrait porter un nouveau coup à l'image de forteresse imprenable qu'Apple essaye de donner à l'iPhone… [Lire la suite]

Source : *iCloud : Apple a essayé d'aider le père de l'enfant mort à récupérer des données – Politique – Numerama*

iPhone chiffré : une boîte israélienne à la rescousse du FBI ?



iPhone chiffré : une boîte israélienne à la rescousse du FBI ?

Lundi 21 mars, le FBI a pris tout le monde de court en annonçant avoir trouvé une solution pour accéder aux données stockées sur l'iPhone chiffré de l'un des co-auteurs de la tuerie de San Bernardino, Syed Farook.
Après avoir aboyé partout que seul Apple pouvait débloquer la situation, l'administration américaine a en effet affirmé avoir reçu l'aide d'un mystérieux « tiers », annulant ainsi une confrontation prévue le lendemain même devant une cour de Californie.
En attendant le compte-rendu de cette méthode, que la justice attend d'ici le 5 avril, la presse spécialisée spécule sur l'identité de l'auxiliaire-mystère. Et avance un nom : Cellebrite.

Maître du « digital forensics »

Pour Yedioth Ahronoth (en hébreu), qui cite des sources anonymes, cela ne fait même aucun doute : c'est bien cette boîte israélienne qui a aidé le FBI.
Vidéo promotionnelle d'une solution de Cellebrite, permettant de débloquer un iPhone
Si les deux intéressés se sont refusés à tout commentaire, les spécialistes de l'informatique et du renseignement estiment l'information probable.
Il faut dire que cette firme, établie depuis 1999, est l'une des rares à maîtriser l'art du « digital forensic » dans la téléphonie mobile et le GPS.
Soit la dissection des appareils numériques, dans le cadre notamment d'enquêtes.
Le chercheur David Billard, sollicité en tant qu'expert dans des affaires de ce genre et rattaché à la cour d'appel de Chambéry, détaille :
« Le digital forensic consiste à récupérer les preuves, ou éléments de preuve, dans des appareils numériques. […]
Par exemple, extraire des vidéos d'un ordinateur dans le cadre d'une enquête sur un viol, retrouver des SMS effacés d'un téléphone portable dans le but de confirmer, ou infirmer, une complicité, etc… »

Analyse des appareils brûlés, écrasés, chiffrés…

*Or en la matière, l'inventaire de Cellebrite est fourni. **Promet de venir à bout** de matériel protégé par un mot de passe, « écrasé, cassé, brûlé ou endommagé par l'eau ». Et, plus intéressant en l'espèce :*
« d'analyser des formats d'application de données et des méthodes de chiffrement complexe et inconnu. »
*Le FBI semble d'ailleurs parfaitement conscient de ces compétences puisque l'agence a noué de nombreux contrats avec Cellebrite, relève le journaliste américain **John Paczkowski**, qui est allé fouiller dans les bases de données publiques de l'administration. A chaque fois, il est question d'acquisition de matériel de télécommunication, sans fil, relatif à l'informatique, par le ministère de la justice américain (le DOJ).*

*L'accord conclu entre Cellebrite et le FBI, le 21 mars 2016 – **DPSD / gouvernement américaine***
*En tout, 2 millions de dollars auraient ainsi été dépensés depuis 2012, **écrit Motherboard**. Qui relève un autre détail intéressant : **le 21 mars 2016**, soit le jour de l'annonce-surprise du FBI, un accord de 15 000 dollars a justement été signé avec Cellebrite.*

Cellebrite déjà sollicité… sans succès

Avant même que le journal israélien pointe explicitement vers Cellebrite, son nom revenait de toute façon déjà dans les articles sur la saga opposant le FBI à Apple.
*L'expert des appareils d'Apple Jonathan Zdziarski **prévenait déjà en septembre 2014** : malgré les précautions louables de la marque, les derniers systèmes d'exploitation de l'iPhone ne sont pas totalement inviolables. Et Cellebrite faisait selon lui parti des rares entreprises capables de fournir des solutions commerciales pour accéder aux données du téléphone.*
*Il ne pouvait être plus proche de la vérité : dans une déclaration remise à la cour appelée à trancher le contentieux entre Apple et le FBI, un ingénieur de l'agence explique avoir déjà eu recours aux services de cette entreprise ! Sans succès… jusque là, **rapporte le New York Times** ce jeudi.*

Nombreux faits d'armes

*Par le passé aussi, Cellebrite s'est démarqué par quelques faits d'armes évocateurs. Début 2016, c'était pour **avoir aidé la police néerlandaise** à lire les messages chiffrés et supprimés d'un Blackberry.*
*Huit ans auparavant, l'association américaine en défense des libertés civiles, l'ACLU, **se lançait dans une procédure** contre la police du Michigan, accusée d'utiliser illégalement les outils de Cellebrite pour fouiller dans les téléphones des suspects.*
*Au nom du Freedom of Information Act (le FOIA), l'organisation **a demandé la publication** de compte-rendus sur l'utilisation de cette solution technique. La police a rétorqué que cette publication lui coûtait des centaines de milliers de dollars et, à notre connaissance, l'ACLU n'a toujours rien reçu… [Lire la suite]*

Réagissez à cet article

Source : *iPhone chiffré : une boîte israélienne à la rescousse du FBI ? – Rue89 – L'Obs*