Furtim, le malware qui détruit les solutions de sécurité.

	Furtim, le malware qui détruit les solutions de sécurité

Alors que de nouveaux malwares sont découverts quasiment chaque jour, voilà que l'un d'entre eux fait beaucoup parler. Il s'agit de Furtim, un #logiciel malveillant qui se caractérise par sa faculté à détruire les solutions de sécurité présentes sur le PC infecté.

Si l'on en croit nos confrères de Silicon, un nouveau malware a été découvert par les équipes d'EnSilo. Comme son nom l'indique, Furtim est capable de passer inaperçu sur les machines qu'il a réussi à infecter.

Probablement crée par des hackers d'Europe de l'Est, ce malware se compose d'un driver qui scanne le PC infecté, d'un module downloader, d'un gestionnaire d'alimentation, d'un voleur de mots de passe et d'un module de communication serveur.

Toutefois, avec une telle composition, impossible de comprendre comment fonctionne réellement ce malware. Pour l'heure, Furtim apparait seulement comme un logiciel malveillant très sophistiqué et capable d'analyser son environnement avant de s'exécuter. Pour cela, il va scanner la machine infectée pour détecter les solutions de sécurité et les outils de filtrage DNS.

Preuve que les pirates ont pensé à tout, Furtim bloque l'accès à de nombreuses sites spécialisés dans la sécurité informatique et à des forums d'aide à la désinfection et désactive les notifications Windows, le gestionnaire des tâches et diverses autres fonctionnalités.

Furtim, un éclaireur en vue de futures attaques

Selon les premières recherches menées par les équipes d'EnSilo, Furtim n'aurait probablement pas vocation à agir seul puisqu'il pourrait bien uniquement jouer un rôle d'éclaireur.

En effet, puisqu'il est capable de déjouer les outils de sécurité, il pourrait être utilisé pour introduire des menaces sur des PC sans que cela ne soit décelable… [Lire la suite]

Réagissez à cet article

Source : *Furtim, le malware qui détruit les solutions de*

sécurité

Auteur : Fabrice Dupuis

---

11 millions volés dans une attaque simultanée de distributeurs automatiques

11 millions volés dans une attaque simultanée de distributeurs automatiques

---

Au Japon, des pirates ont réussi à dérober 1,4 milliard de yens (11 millions d'euros) à partir de 1.400 distributeurs automatiques à travers le pays en seulement deux heures. Cette affaire intrigue sérieusement la police japonaise. Des malfaiteurs sont parvenus à voler 1,4 milliard de yens (11 millions d'euros) à partir de 1.400 distributeurs automatiques de billets différents. L'affaire était dans le sac en moins de deux heures.

Cartes contrefaites

Ce vol a probablement été mené par un groupe international faisant usage de cartes de crédit contrefaites contenant des informations de compte dérobées à une banque sud-africaine. Le nom de la banque n'a pas été mentionné et Interpol compte bien aider la police nippone dans cette affaire, comme le rapporte The Japan Times. 14.000 transactions Plus de 100 personnes pourraient avoir coordonné ce retrait d'argent colossal. Le montant maximal de 100.000 yen a été retiré dans chacune des 14.000 transactions…. [Lire la suite]

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

M

Réagissez à cet article

Source : *(Mobile) – 11 millions volés dans une attaque simultanée de distributeurs automatiques*

Cybersécurité en Afrique : état des lieux et perspectives

Cybersécurité en Afrique : état des lieux et perspectives

Avec 20% de de sa population connectée à Internet, l'Afrique est un continent en voie de connexion au cyberespace. Une partie des pays du continent profite des retombées économiques du numérique mais ceux-ci doivent aussi faire face aux cybermenaces qui mettent en péril leur développement dans le cyberespace. Dès lors, comment se construit la cybersécurité en Afrique?

L'ENJEU DE LA CONNECTIVITÉ AVANT CELUI DE LA CYBERSÉCURITÉ

Avant d'évoquer pleinement la question de la cybersécurité en Afrique, il convient au préalable de poser une série de constats sur le niveau de connectivité du continent africain… [Lire la suite]

Article original : *Cybersécurité en Afrique : état des lieux et perspectives – SOLUCOMINSIGHT*
Auteur : JULIEN DOUILLARD Consultant

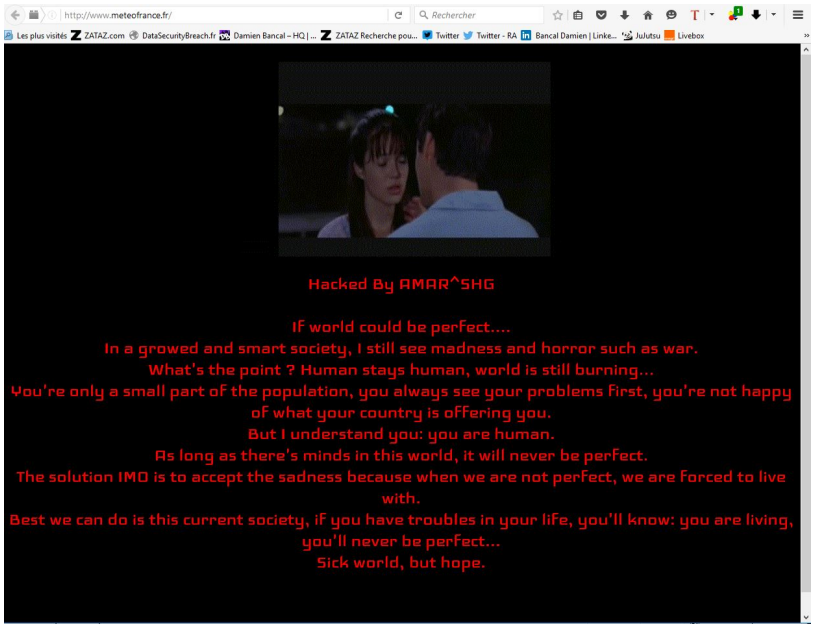
Réagissez à cet article

Le site Internet de Météo France victime de détournement de DNS après celui de Canal +

M

Le site Internet de Météo France victime de détournement de DNS après celui de Canal +

Après les sites de Canal +, un nouveau message d'espoir mis en ligne par un pirate informatique sur l'ensemble des sites Internet de Météo France. Un détournement de DNS radical.



Il se nomme Amar^SHG. Ce jeune pirate informatique (Il serait un Albanais) est dans la mouvance des hacktivistes politiques qui, par le biais de la modification de site Internet (defacement, barbouillage), trouvent un moyen de faire passer des messages. Amar^SHG a fait la pluie et le beau temps sur les sites de Météo France via un détournement de DNS radical.
Lundi soir, le pirate a mis la main sur un moyen informatique qui lui a donné l'occasion de détourner l'ensemble des noms de domaines de Météo France. Comme il a pu me l'indiquer sur Twitter, les domaines .fr, .mobi, . Paris, … ont été impactés.

Détournement de DNS

Les visiteurs accédaient, ce lundi soir (vers 22h30), à une page noire et rouge, portée par la musique « Wonderful life » de Katie Melua. Côté message, le cyber manifestant souhaitait viser ceux qui « se plaignent pour leurs propres problèmes ». AMAR ^ SHG parle d'espoir, d'un monde qui n'est pas parfait « Il faut vivre avec, avec espoir ».
Un message qui change des propos de haines, guerriers… que l'on peut croiser sur des pages modifiées par d'autres pirates informatiques. Une attaque qui a pu être mise en place via un phishing, un accès non autorisés à partir d'une injection SQL… Bref, plusieurs méthodes possibles ont pu être exploitées pour atteindre l'administration des noms de domaine et orchestrer ce détournement de DNS… [Lire la suite]

Réagissez à cet article

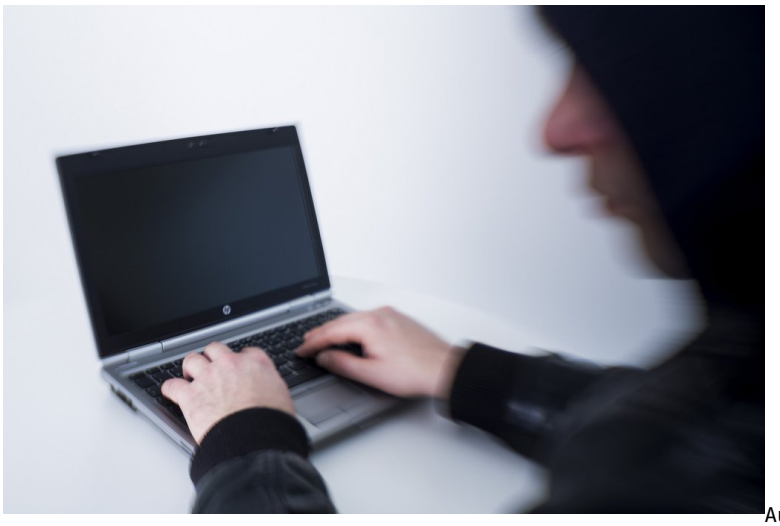
Source : *ZATAZ Détournement de DNS – Un pirate passe par Météo France – ZATAZ*

La cybercriminalité fait des ravages dans les entreprises françaises.

La cybercriminalité fait des ravages dans les entreprises françaises

---

Selon une étude du cabinet PwC, le nombre d'entreprises françaises victimes de la cybercriminalité a presque doublé en deux ans.



Au cours des 2 dernières années, près de 70% des entreprises françaises ont été victimes de fraudes. On note notamment une forte hausse de la cybercriminalité, selon une étude effectuée par le cabinet Price Water House Coopers (PwC) publiée hier. La moyenne nationale est beaucoup plus élevée que celle mondiale.

La cybercriminalité visant les entreprises françaises explose

Les entreprises françaises sont-elles des cibles faciles pour les pirates ? Selon une étude de Price Water House Coopers concernant les fraudes en entreprises, les attaques informatiques occupent le deuxième rang derrière le détournement d'actifs. En 2 ans, la cybercriminalité a explosé en France, elle représente 53% des fraudes en 2016 contre 28% en 2014.

Aujourd'hui, une grande partie des entreprises (85%) ont pris conscience que le risque d'être victime de pirates informatiques est bel et bien réel. Elles n'étaient que 48% en 2014. Selon Louis Di Giovanni, travaillant dans le département Litiges et Investigations du cabinet PwC, « L'explosion du Big Data quels que soient les domaines, alliée à la digitalisation de l'activité économique et la multiplicité des supports numériques augmentent l'exposition des entreprises au risque de cyberattaque, d'où une plus grande prise en compte de ce risque par les dirigeants« .

Les entreprises françaises ne sont pas prêtes face à ce risque

Bien que les entreprises françaises aient bien pris en compte le risque élevé que représente la cybercriminalité, elles n'ont pas forcément mis en place de défenses adéquates. « Plus de la moitié des entreprises françaises n'ont pas encore de plan d'action 100% opérationnel pour répondre à une cyberattaque » déclarait M. Di Giovanni.

A cause de l'explosion de la cybercriminalité, le taux de fraude en entreprise progresse fortement. 68% des entreprises ont déclaré avoir été victimes d'une fraude au cours des deux dernières années, contre 55% en 2014, soit une hausse de 13 points… [Lire la suite]

L'étude PWC Global Economic Crime Survey 2016

Réagissez à cet article

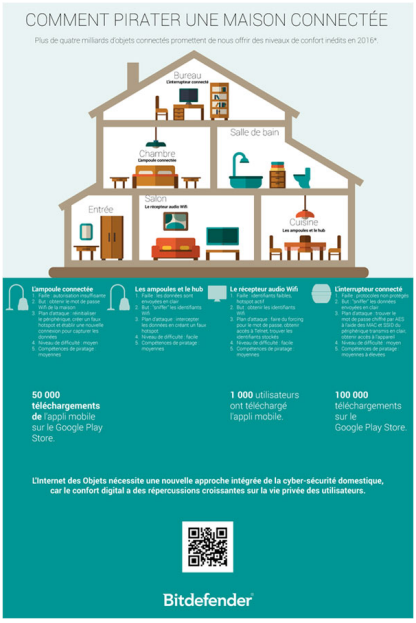
Source : *La cybercriminalité fait des ravages dans les entreprises françaises*

Auteur : David Pain

Est-ce facile de pirater une maison connectée ?

	**Est-ce facile de pirater une maison connectée ?**

L'analyse révèle que les mécanismes d'authentification de ces objets connectés peuvent être contournés et donc exposer potentiellement les foyers et leurs occupants à une violation de leur vie privée. L'Internet des Objets pose des problèmes de sécurité spécifiques, et par conséquent, nécessite une nouvelle approche intégrée de la cyber-sécurité domestique, qui passe de la sécurité centrée sur le périphérique à une solution capable de protéger un nombre illimité d'appareils et d'intercepter les attaques là où elles se produisent : sur le réseau.



Les chercheurs des Bitdefender Labs ont réalisé une étude sur quatre périphériques de l'Internet des Objets (IdO) destinés au grand public, afin d'en savoir plus sur la sécurisation des données de l'utilisateur et les risques dans un foyer connecté :

1. **L'interrupteur connecté WeMo Switch** qui utilise le réseau WiFi existant pour contrôler les appareils électroniques (télévisions, lampes, chauffages, ventilateurs, etc.), quel que soit l'endroit où vous vous trouvez ;
2. **L'ampoule LED Lifx Bulb** connectée via WiFi, compatible avec Nest ;
3. Le kit **LinkHub**, incluant des**ampoules GE Link et un hub** pour gérer à distance les lampes, individuellement ou par groupes, les synchroniser avec d'autres périphériques connectés et automatiser l'éclairage selon l'emploi du temps ;
4. **Le récepteur audio Wifi Cobblestone de Muzo** pour diffuser de la musique depuis son smartphone ou sa tablette, via le réseau WiFi.

L'analyse révèle que les mécanismes d'authentification de ces objets connectés peuvent être contournés et donc exposer potentiellement les foyers et leurs occupants à **une violation de leur vie privée**. Les chercheurs de Bitdefender sont parvenus à découvrir le mot de passe pour accéder à l'objet connecté et à intercepter les identifiant et mot de passe WiFi de l'utilisateur.

Les **failles identifiées** par l'équipe de recherche Bitdefender concernent des protocoles non protégés et donc vulnérables, des autorisations et authentifications insuffisantes, un manque de chiffrement lors de la configuration via le hotspot (données envoyées en clair) ou encore des identifiants faibles.

L'IdO pose des problèmes de sécurité spécifiques, et par conséquent, nécessite **une nouvelle approche intégrée de la cyber-sécurité domestique**, qui passe de la sécurité centrée sur le périphérique à une solution capable de protéger un nombre illimité d'appareils et d'intercepter les attaques là où elles se produisent : **sur le réseau**.

Si des marques comme Philips et Apple ont créé un écosystème verrouillé, **l'interopérabilité reste essentielle** à ce stade du développement des nouveaux objets connectés. Il est donc plus que temps que les constructeurs prennent en compte nativement la sécurité dans le développement de leurs différents appareils… [Lire la suite]

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

Source : *Comment pirater une maison connectée ?*

Victime du ransomware

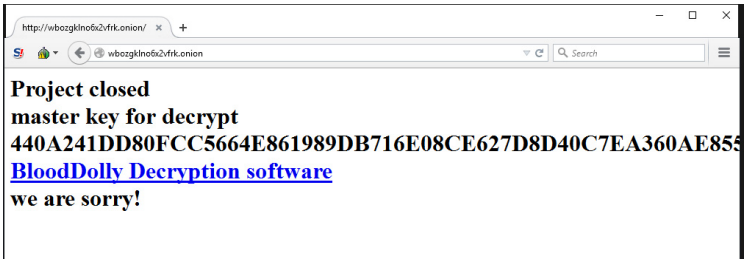
TelsaCrypt ? Voici finalement la clé de déchiffrement

	Victime du ransomware TelsaCrypt ? Voici finalement la clé de déchiffrement

Les auteurs du ransomware TeslaCrypt ont décidé de réparer leurs méfaits en fournissant gracieusement la clé qui permet aux victimes du logiciel d'extorsion de reprendre le contrôle sur leurs données.

Les maître-chanteurs des temps modernes auraient-ils aussi parfois une conscience, qui se réveille tardivement ? Depuis de nombreux mois, des groupes de délinquants anonymes inondaient des systèmes informatiques d'un ransomware basé sur le framework TeslaCrypt, à l'action hélas désormais bien connue. La victime se retrouvait avec tous ses fichiers et documents personnels chiffrés sur son disque dur, et le seul moyen de les déchiffrer pour y avoir de nouveau accès était de payer une rançon, en suivant les instructions affichées à l'écran. Mais l'auteur (ou les auteurs ?) de TeslaCrypt a décidé de faire amende honorable.

L'éditeur de logiciels de sécurité ESET avait en effet remarqué que les créateurs de TeslaCrypt avaient choisi de mettre fin à leur projet maléfique. Prenant leur audace à deux mains, les ingénieurs du groupe ont donc contacté les créateurs de TeslaCrypt en passant par le service d'assistance intégré au ransomware, et leur ont demandé s'ils accepteraient de publier la « master key » qui permettrait à toutes les victimes de déchiffrer leurs fichiers sans payer un centime.
À leur propre surprise, les pirates ont accepté. La clé est désormais visible sur le site du groupe (accessible uniquement en passant par Tor).



« *Nous sommes désolés* », peut-on lire sur ce site, qui donne également le lien vers un outil de déchiffrement mis au point par BloodDolly, présenté par BleepingComputer comme un « expert de TeslaCrypt ». Il avait déjà proposé un outil gratuit pour déchiffrer les fichiers bloqués par TeslaCrypt 1.0, mais la communication de la clé maître permet désormais à l'outil de déchiffrer y compris TeslaCrypt 3.0 et TeslaCrypt 4.0. ESET a également publié son propre outil gratuit.
L'histoire ne dit pas pourquoi les auteurs du ransomware ont été pris de remords… [Lire la suite]

Réagissez à cet article

Source : *Les auteurs du ransomware TelsaCrypt s'excusent et offrent la clé – Tech – Numerama*

Avec l'intelligence artificielle, Facebook en sait autant sur vous que votre conjoint

	Avec l'intelligence artificielle, Facebook en sait autant sur vous que votre conjoint. – Entreprises Numériques

---

Impossible d'échapper aux mécanismes de recommandations sur Internet. Tous les sites internet, marchands ou réseaux sociaux, utilisent désormais ces fameuses recommandations censées influencer nos comportements d'achats. Basées sur de l'intelligence artificielle de plus en plus puissante, les recommandations se font plus pertinentes. Dans l'avenir elles pourront tirer profit d'une connaissance précise de notre personnalité comme le montre une étude réalisée à partir de l'analyse des « likes » de Facebook.

Toute action sur Internet se transforme en données. On s'inquiète à juste titre de l'usage qui est fait de nos données personnelles (voir mon billet sur Safe Harbor). L'annonce par Facebook de « Search FYI » devrait encore attirer notre attention sur la protection de notre vie privée. Avec Search FYI, Facebook peut rechercher des informations dans tous les messages publics publiés par ses membres. Avec le développement de l'intelligence artificielle et l'utilisation du machine learning la valeur des données monte en flèche. Le mot « donnée » est souvent sous-estimé. On comprend bien qu'une photo et un texte postés sur un réseau social sont des données mais on oublie que le simple fait de cliquer sur un « like » devient une donnée aussi importante voire plus. Toute action sur internet laisse une trace numérique qui pourra être exploitée. C'est la base même du marketing digitale qui utilise ces traces numériques laissées sur le parcourt client pour mieux connaitre le consommateur et augmenter l'expérience utilisateur. C'est du donnant donnant : mieux nous sommes connus, mieux nous sommes servis. C'est l'évolution naturelle liée à la transformation numérique.
En analysant les « Likes », Facebook en sait plus sur notre personnalité que nos proches. La personnalité est un concept complexe qui semble difficilement mesurable. Cela touche à des sentiments, des émotions, des valeurs qui nous façonnent et qui nous rendent uniques. On pourrait donc imaginer, voire espérer, que les ordinateurs puissent se montrer impuissants à « quantifier » ce qui nous définit en tant qu'être humain. Pourtant une étude menée par des chercheurs des universités de Cambridge et de Stanford, publiée en janvier 2015, a montré que l'Intelligence Artificielle a le potentiel de mieux nous connaitre que nos proches. Cette étude visait à comparer la précision d'un jugement sur la personnalité réalisé par un ordinateur et des êtres humains. Les chercheurs ont demandé à 86.200 volontaires de leur donner accès à leurs « Likes » sur Facebook et de répondre à un questionnaire de 100 questions sur leur personnalité. Ces données ont été modélisées et le résultat est assez étonnant. On apprend que :
Avec l'analyse de 10 likes, Facebook en sait plus sur nous que nos collèges
Avec 70 likes Facebook en sait plus que nos amis
Avec 150 likes Facebook en sait plus que notre famille
Avec 300 likes Facebook en sait plus que notre conjoint
Quand on sait qu'en moyenne un utilisateur Facebook a 227 Likes, on se dit que nous n'avons plus grand choses à cacher.
Partager des émotions comme on partage des photos ou des vidéos. C'est la prochaine étape qu'imagine Mark Zuckerberg dans le futur. Durant une session de questions réponses sur son profile Facebook, le patron de Facebook a expliqué qu'il pensait que nous aurions à l'avenir la possibilité de partager nos expériences émotionnelles rien que par le seul fait d'y penser. La télépathie appliquée aux réseaux sociaux ? En matière d'Intelligence artificielle il devient difficile de faire la différence entre science-fiction et prévision. Quoiqu'il en soit Gartner a rappelé que c'étaient les algorithmes qui donnaient leur valeur aux données. Le progrès de ces algorithmes et leur complexité justifient qu'on s'intéresse à la protection de notre vie privée. Ils deviennent incontournables dans notre vie moderne, il faut en être conscient… [Lire la suite]

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

Source : *Avec l'intelligence artificielle, Facebook en sait autant sur vous que votre conjoint. – Entreprises Numériques*

Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google

Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google

---

Le lanceur d'alerte à l'origine du scandale de la surveillance de la NSA et des spécialistes en sécurité informatique mettent en cause la politique de chiffrement mise en place par Google pour sa nouvelle messagerie.

Haro sur Allo. La nouvelle application de messagerie instantanée de Google était l'une des principales annonces de la conférence Google I/O, mercredi 18 mai, au quartier général de l'entreprise à Mountain View. Fondée sur l'intelligence artificielle, elle est capable de comprendre le langage humain et affine son algorithme au fil des conversations afin de proposer des suggestions de plus en plus pertinentes. Disponible cet été sur Android et iOS, elle est déjà au coeur d'une controverse d'experts.
Allo possède des paramètres de sécurité renforcés. Un mode « incognito » permet de chiffrer de bout en bout les messages afin de les rendre illisibles pour une personne extérieure à la conversation. Seuls les participants à la discussion sont en mesure de les déchiffrer. Google lui-même ne peut pas y accéder et répondre à d'éventuelles requêtes judiciaires des autorités.
Cette option est basée sur le protocole open source Signal, développé par Open Whispers Systems. C'est le même protocole de chiffrement que WhatsApp, dont les discussions sont cryptées de bout en bout depuis le mois d'avril. Mais à l'inverse de WhatsApp et d'autres messageries sécurisées actuelles (Viber, Signal, iMessage) le chiffrement des conversations n'est pas activé par défaut sur Allo. C'est aux utilisateurs d'effectuer la démarche.

Les experts en sécurité déconseillent Allo

Des experts en cybersécurité s'interrogent déjà sur la pertinence d'une telle fonction, arguant que de nombreux utilisateurs ne feront pas la démarche de l'activer. « La décision de Google de désactiver par défaut le chiffrement de bout en bout dans la nouvelle application de discussion instantanée Allo est dangereuse et la rend risquée. Évitez-la pour l'instant », a conseillé Edward Snowden sur Twitter.
Le lanceur d'alerte à l'origine du scandale des programmes de surveillance de la NSA en 2013 n'est pas le seul à critiquer le choix de Google. Nate Cardozo, représentant de l'EFF, une association américaine de défense des libertés numériques, a estimé pour sa part que « présenter la nouvelle application de Google comme étant sécurisée n'est pas juste. L'absence de sécurité par défaut est l'absence de sécurité tout court ».
« Rendre le chiffrement optionnel est une décision prise par les équipes commerciales et juridiques. Elle permet à Google d'exploiter les conversations et de ne pas agacer les autorités », a encore indiqué Christopher Soghoian, membre de l'Association américaine pour les liberté civiles.

L'intelligence artificielle, priorité de Google

Après avoir pris fait et cause pour Apple dans le bras de fer qui l'a opposé au FBI sur le déblocage de l'iPhone chiffré d'un des terroristes de San Bernardino, Google n'est donc pas allé aussi loin que WhatsApp en généralisant le chiffrement des discussions. Un ingénieur en sécurité de Google a expliqué sur son blog comment la société avait dû arbitrer entre la sécurité des utilisateurs et les services d'intelligence artificielle d'Allo.
Pour profiter pleinement des capacités de Google Assistant implémentées dans Allo, les algorithmes doivent être en mesure d'analyser les conversations, ce qui n'est possible qu'en clair. « Dans le mode normal, une intelligence artificielle lit vos messages et utilise l'apprentissage automatique pour les analyser, comprendre ce que vous voulez faire et vous donner des suggestions opportunes et utiles », explique Thaï Duong.
Ce parti pris pourrait évoluer d'ici la sortie de l'application cet été. Le site américain TechCrunch a publié des paragraphes que l'ingénieur avait publié dans son article avant de les supprimer. Il affirme qu'il est en train de « plaider en faveur d'un réglage avec lequel les usagers peuvent choisir de discuter avec des messages en clair », pour interagir avec l'intelligence artificielle en l'invoquant spécifiquement, sans renoncer à la vie privée. En somme, proposer « le meilleur des deux mondes »… [Lire la suite]

Source : *Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google*

Pourquoi la vidéosurveillance de Salah Abdeslam pose question légalement ?

Pourquoi la vidéosurveillance de Salah Abdeslam pose question légalement ?

Arrêté en Belgique le 18 mars 2016 suite aux attentats de Paris du 13 novembre 2015, Monsieur Salah Abdeslam a été mis en examen notamment pour assassinats et tentatives d'assassinats en bande organisée en relation avec une entreprise terroriste, et placé en détention provisoire le 27 avril à la maison d'arrêt de Fleury Mérogis, dans l'attente de son jugement.

Il est aujourd'hui placé en isolement total dans une cellule de 9m2, et deux caméras le filment 24h/24. Cette mesure, tout-à-fait exceptionnelle, est justifiée, selon le Ministre de la Justice français, "conformément aux exigences la Convention Européenne de Sauvegarde des Droits de l'Homme et du droit français de la protection des données personnelles".
La loi française prévoit un régime dérogatoire s'agissant de la procédure pénale en matière de terrorisme, mais aucune disposition n'envisage spécifiquement la mise en place d'un dispositif de surveillance continue de la cellule d'un détenu. La Cour Suprême française (Cour de Cassation) a retenu à une reprise, en matière de criminalité organisée, la validité de la sonorisation permanente d'une cellule, sur autorisation du juge d'instruction.
Un arrêté français du 23 décembre 2014 autorise le contrôle sous vidéoprotection d'une cellule de protection d'urgence, mais ce texte ne vise que les détenus "dont l'état apparaît incompatible avec leur placement ou leur maintien en cellule ordinaire en raison d'un risque de passage à l'acte suicidaire imminent ou lors d'une crise aigüe" et alors la durée d'enregistrement ne peut dépasser 24 heures consécutives. C'est dans l'une de ces cellules de protection d'urgence pour les détenus suicidaires que monsieur Salah Abdeslam est actuellement détenu. L'arrêté ne serait donc applicable que s'il était démontré un risque imminent de passage à l'acte suicidaire, alors que Monsieur Salah Abdeslam est isolé, ses visites étant très limitées, et complètement isolé des autres détenus à chaque promenade. Il dispose en outre d'un pyjama en papier, sa cellule vide faisant l'objet d'une surveillance accrue par des rondes renforcées toutes les 3 heures. Monsieur Salah Abdeslam lui-même est encadré par une équipe de surveillants et médecins spécialisés dans les personnes dangereuses.
La Cour Européenne des Droits de l'Homme a permis aux détenus de bénéficier d'une véritable protection de leurs droits, en s'appuyant notamment sur l'article 3 de la convention, relatif aux traitements inhumains et dégradants. Les états membres doivent en effet s'assurer que la détention est compatible avec le respect de la dignité humaine et à veiller à ce que la santé et le bien-être du prisonnier soient assurés de manière adéquate. La Cour a déjà tenu compte, dans une affaire d'isolement carcéral et dans un contexte de la lutte contre le terrorisme, de la personnalité du détenu et de sa dangerosité hors norme, pour justifier de la mise en place de telles mesures (CEDH Grande Chambre, 4 juillet 2006, Ramirez Sanchez c/ France).
En matière de vidéosurveillance continue, la Cour Européenne a déjà été saisie de cette question, mais n'y a pas répondu, estimant que le requérant n'avait pas épuisé toutes les voies de recours internes dont il bénéficiait pour contester l'application de la mesure de sa vidéosurveillance (CEDH, Riina c/ Italie, 11 mars 2014). Le requérant, condamné à la réclusion à perpétuité pour association de malfaiteurs de type mafieux et de multiples assassinats se plaignait d'une vidéosurveillance constante dans sa cellule, y compris dans les toilettes.
Conscient de ce vide juridique, le Ministère de la Justice français a saisi l'autorité française de contrôle et de protection des données personnelles (CNIL), en charge notamment des questions liées la conservation des enregistrements et des mesures de vidéoprotection, d'un projet d'arrêté sur la vidéosurveillance en prison. Son avis sera rendu public dans les prochains jours.
En cas d'avis défavorable de la CNIL, l'avocat de Salah Abdeslam serait en droit de contester la mesure et de réclamer, outre une réduction de la mesure de vidéoprotection, une indemnisation financière devant le directeur de la prison, et en cas de rejet, de saisir le juge administratif français d'un recours. A charge pour l'avocat d'inscrire cette procédure de contestation dans une stratégie de défense plus générale… [Lire la suite]

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

Source : *Pourquoi la vidéosurveillance 24h/24 de Salah Abdeslam pose question légalement*