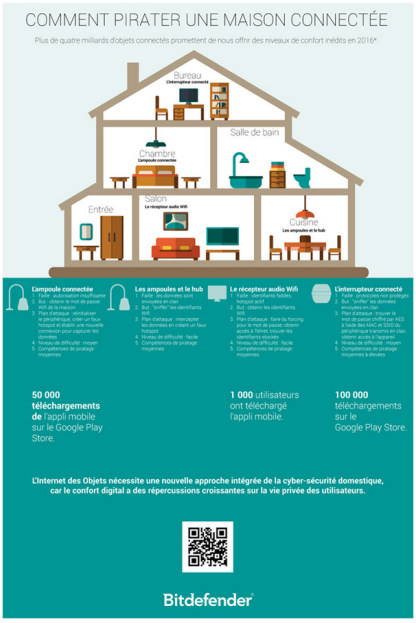
Est-ce facile de pirater une maison connectée ?

	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

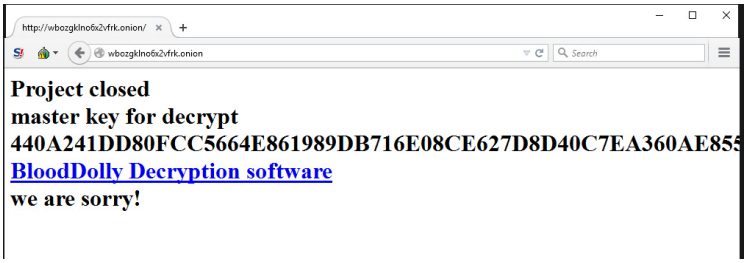
TelsaCrypt ? Voici finalement la clé de déchiffrement

	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*

Entreprises, surveillez l'usage des réseaux sociaux !

Entreprises, surveillez l'usage des réseaux sociaux !

Selon Osterman Research, près de une entreprise sur cinq a été victime de malwares diffusés par le biais de réseaux sociaux.

Les réseaux sociaux sont des outils de communication clés pour les entreprises, mais ils constituent aussi un vecteur d'attaques informatiques encore trop souvent négligé par les organisations, observe le cabinet américain Osterman Research dans un livre blanc (Best Practices for Social Media Archiving and Security). Sponsorisée par Actiance, Gwava et Smarsh, l'enquête a été réalisée auprès d'un panel de professionnels IT et décideurs d'entreprises de taille moyenne et de grands groupes.
73 % des entreprises concernées par cette enquête utilisent Facebook dans le cadre professionnel, 64 % LinkedIn et 56 % Twitter. Plusieurs plateformes sont utilisées régulièrement. Du côté des réseaux sociaux d'entreprise (RSE), Microsoft Sharepoint est l'outil le plus largement cité (par 82 % des répondants). Il devance Jabber et WebEx de Cisco ou encore Yammer de Microsoft.

Une porte d'entrée pour les malwares
54 % des organisations ont adopté une politique relative à l'utilisation par leurs collaborateurs des réseaux sociaux tout public (ce taux passe à 51 % pour les RSE). Mais elles ne sont plus que 48 % à le faire lorsqu'il est question de l'usage professionnel des plateformes tout public. Si une majorité veille ou surveille cet usage, 27 % ne le font pas. Et ce malgré les cybermenaces et les risques juridiques auxquels les entreprises sont confrontées.
Dans ce contexte, 18 % ont constaté que leur compte « social » a été piraté ou ont été victime d'une attaque par malware, soit près d'un utilisateur de réseau social sur cinq en entreprise. Mais pour 80 % des répondants, c'est bien l'email qui constitue la première source d'infiltration de logiciels malveillants dans les systèmes et réseaux internes des organisations
[Lien vers l'article original partagé]

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 : *Sécurité : entreprises, surveillez l'usage des réseaux sociaux !*

Google fait semblant de ne rien comprendre à ce qu'exige la Cnil

Google fait semblant de ne rien comprendre à ce qu'exige la Cnil

---

Source : *Droit à l’oubli : Comment Google feint de ne rien comprendre à ce qu’exige la Cnil – Politique – Numerama*

Tout sur les arnaques et les piratages Informatiques sur @LCI ce 23 mai 2016 en direct de 9h15 à 10h avec Denis JACOPINI

Tout sur les arnaques et les piratages Informatiques sur @LCI ce 23 mai 2016 en direct de 9h15 à 10h avec Denis JACOPINI

Denis JACOPINI sera ce lundi 23 mai 2016 en direct sur LCI pour vous parler pendant près d'une heure des mails malveillants, des arnaques où les pirates se font passer pour EDF ou les impôts pour soutirer les données bancaires…

Le but de cette émission sera avant tout sera d'expliquer le phénomène en croissance incoercible de la cybercriminalité.
A cours de l'émission nous verrons les pièges à éviter, et quelques conseils à suivre pour se protéger des pirates informatiques.
Suivez le direct sur lci.tf1.fr

Le replay sera mis en ligne dans les jours qui suivront et accessible aussi sur cette page.

Vous pouvez également découvrir toutes les solutions de notre expert lors de ses formations et actions de sensibilisation à la cybersécurité, au piratage informatique, aux arnaques pour mieux vous en protéger.

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 : *Ransomware*

Plus de 100 millions de mots de passe LinkedIn dans la nature… depuis 2012 !

	**Plus de 100 millions de mots de passe LinkedIn dans la nature… depuis 2012 !**

Une base de données, contenant 117 millions de combinaisons d'identifiants et de mots de passe, est vendue 2000 euros par des pirates. Le réseau social professionnel enquête.

Le piratage massif dont a été victime LinkedIn en 2012 revient hanter le réseau social professionnel. Une base de données contenant plus de 100 millions d'identifiants et de mots de passe est actuellement proposée à la vente sur une place de marché du dark web, «The Real Deal», rapporte le siteMotherBoard. Le fichier est proposé à la vente pour 5 bitcoins, soit un peu plus de 2000 euros. Il concerne 167 millions de comptes, dont 117 millions sont associés à un mot de passe.

Le site LeakedSource, qui a eu accès au fichier, assure avoir réussi à déchiffrer en trois jours «90% des mots de passe». Ils étaient en théorie protégés par un procédé de hachage cryptographique, SHA-1, mais sans salage, une technique compliquant leur lecture en clair. Deux personnes, présentes dans le fichier, ont confirmé à un chercheur en cybersécurité que le mot de passe associé à leur identifiant était authentique.

LinkedIn avait reconnu en 2012 le vol des données de connexion, mais sans jamais préciser le nombre d'utilisateurs concernés. Un fichier, concernant 6,5 millions de comptes, avait à l'époque été mis en ligne. «À l'époque, notre réponse a été d'imposer un changement de mot de passe à tous les utilisateurs que nous pensions touchés. De plus, nous avons conseillé à tous les membres de LinkedIn de changer leurs mots de passe», commente aujourd'hui le réseau social professionnel sur son blog.

123456, linkedin, password, 123456789 et 12345678

En réalité, un porte-parole de LinkedIn avoue «ne pas savoir combien de mots de passe ont alors été récupérés». «Nous avons appris hier qu'un jeu de données supplémentaire qui porterait supposément sur plus de 100 millions de comptes et proviendrait du même vol de 2012, aurait été mis en ligne. Nous prenons des mesures immédiates pour annuler ces mots de passe et allons contacter nos membres. Nous n'avons pas d'éléments qui nous permettent d'affirmer que ce serait le résultat d'une nouvelle faille de sécurité», ajoute LinkedIn sur son blog.

Selon LeakedSource, la base de données aurait été détenue jusqu'alors par un groupe de pirates russes. Ces informations de connexion, même si elles remontent à 2012, ont encore une grande valeur. Elles peuvent être utilisées tout à la fois pour pénétrer dans d'autres comptes plus critiques (sites d'e-commerce, banque en ligne…) ou organiser des campagnes de phishing, une technique utilisée pour obtenir les renseignements personnels d'internautes. Nombre d'utilisateurs utilisent la même combinaison d'adresse email et de mot de passe sur tous les sites, et en changent peu souvent, ce qui démultiplie les effets de tels piratages.Preuve de cette imprudence générale, les cinq mots de passe les plus utilisés dans le fichier mis en vente étaient 123456, linkedin, password, 123456789 et 12345678… [Lire la suite]

Réagissez à cet article

Source : *Plus de 100 millions de mots de passe LinkedIn dans la nature*

Prise d’otage numérique par Rançongiciels, la nouvelle arme fatale des cyberpirates

Prise d’otage numérique par Rançongiciels, la nouvelle arme fatale des cyberpirates

---

Les prises d'otages numériques, avec demande de rançon, se multiplient. Payer est souvent la seule solution

Locky, Cryptolocker, Synolocker, Cryptowall, TeslaCrypt, Petya… Si vous n'êtes pas un spécialiste de la sécurité informatique, ces noms barbares ne vous disent probablement rien. Et pourtant, ils représentent la nouvelle menace qui pèse sur vos ordinateurs. Depuis quelques années, en effet, un nouveau type de logiciel malveillant a le vent en poupe: les rançongiciels – un néologisme 2.0 dérivé du mot «ransomware» dans la langue de Shakespeare. Ces virus prennent, à distance, le contrôle de PC, tablettes ou smartphones et bloquent l'ensemble de leurs données. Pour les récupérer, les propriétaires légitimes sont sommés de payer une rançon dans un délai très court, dans une monnaie virtuelle et non traçable comme les bitcoins.
Selon une étude d'Intel Security-McAffe, datant de mars 2016, ce type d'attaque a augmenté de 26% au dernier trimestre 2015, par rapport à l'année précédente.

Les PME ne sont pas préparées

«Les demandes de rançons après un piratage sont en plein essor dans le monde et en Suisse, résume Ilia Kolochenko, CEO et fondateur de l'entreprise genevoise High-Tech Bridge, spécialisée dans la sécurité informatique. C'est devenu une véritable industrie.»
De fait, les exemples se multiplient – proches de nous. En avril 2016 par exemple, Ralph Eberhard, patron de la gérance Immogeste basée à Genève, témoigne dans le journal *Le Temps* avoir dû payer 1000 francs à des hackers. Le même mois, un peu plus loin d'ici, dans le Béarn, le PDG d'une entreprise raconte peu ou prou la même histoire, dans le journal *La République des Pyrénées*.
En effet, à chaque fois le scénario est identique. Un matin, en allumant leurs ordinateurs, les salariés voient s'afficher sur leur moniteur un message martial, généralement rouge sur fond noir, qui dit en substance: «Tous les fichiers de votre disque dur ont été cryptés. Pour les déchiffrer et les récupérer, vous devez nous payer.» La plupart du temps, les montants exigés ne s'avèrent pas dissuasifs: de quelques centaines de francs pour des particuliers à quelques milliers pour les PME. Mais parfois les sommes demandées sont astronomiques. En février 2016, un ransomware a infecté un hôpital de Los Angeles, bloquant l'ensemble des données médicales des patients. Pour remettre le système d'information d'aplomb, les pirates ont réclamé 9000 bitcoins, soit l'équivalent de 3,6 millions de dollars!
«Auparavant, les hackers s'attaquaient à de grosses entreprises, afin de toucher le jackpot, rappelle Ilia Kolochenko. Aujourd'hui, ils se recentrent sur les PME et les particuliers, parce qu'ils ont compris que même si les sommes obtenues sont moindres, l'activité se révèle moins risquée et plus facile. Si vous attaquez une grande banque, vous devez d'abord déjouer une sécurité informatique de premier plan. Et si vous y parvenez, vous pouvez être certain qu'elle ne vous lâchera jamais. Elle vous traquera pendant des années s'il le faut. A l'inverse, les particuliers et les PME ne sont absolument pas préparés à ce type d'attaque et en plus ne disposent pas des moyens nécessaires pour retrouver les auteurs.» Selon un rapport de Symantec publié en avril 2016, 57% de ces attaques ciblent des entreprises de moins de 250 salariés.
Mais comment ces logiciels malveillants se diffusent-ils? «Ces chevaux de Troie accèdent à l'ordinateur par le biais de courriels infectés ou de sites Internet piratés», explique la centrale Melani. Concrètement, «les hackers possèdent des robots informatiques, les botnets, qui scrollent l'ensemble des pages Internet – un peu comme Google – à la recherche de failles connues, explique Ilia Kolochenko. Lorsqu'une vulnérabilité est découverte, le virus s'installe et attend sa victime, en affichant par exemple un nouveau lien. Lorsque quelqu'un clique sur ce dernier, le virus passe sur son ordinateur et crypte l'ensemble des données.»

Faut-il payer la rançon ou pas?

Face à cette situation, la centrale Melani recommande de «ne pas céder à l'extorsion car, en payant la rançon, vous participez au financement de l'activité des criminels et leur permettez d'améliorer l'efficacité de leurs prochaines attaques. De plus, il n'existe aucune garantie que les criminels respecteront leur engagement et vous enverront réellement la clé vous permettant de récupérer vos données.»
En pratique, les choses s'avèrent plus compliquées, notamment pour les PME qui, privées de leurs fichiers clients, voient toute leur activité bloquée. «Si vous êtes infectés, il n'existe pas 3000 solutions, reconnaît Ilia Kolochenko. La première consiste à faire des recherches sur Internet, afin de savoir s'il existe déjà une clef de décryptage contre le rançongiciel. Malheureusement, c'est rarement le cas. La seconde, c'est payer. Si vous vous adressez à une entreprise comme la nôtre, nous finirons par remonter jusqu'au coupable et nous parviendrons peut-être à récupérer vos données. Mais cela va prendre beaucoup de temps. Même si cela peut paraître immoral, c'est moins coûteux pour une PME de régler la rançon que de lancer des investigations.» (TDG)
_ [Lire la suite]

Réagissez à cet article

Source : *Sécurité informatique: Rançongiciels, la nouvelle arme fatale des cyberpirates – News High-Tech: Hard-/Software – tdg.ch*