Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue

	Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue

Les chercheurs d'ESET découvrent un malware qui a échappé à la surveillance des chercheurs d'antivirus depuis au moins 2008. Ce malware, nommé Win32/Prikormka et détecté par ESET comme malware utilisé pour mener des activités de cyber-espionnage, cible principalement les séparatistes anti-gouvernementaux des républiques autoproclamées de Donetsk et Luhansk.

« Avec la crise ukrainienne de l'EST du pays, ce dernier a connu de nombreuses cyber-attaques ciblées ou de menaces persistantes avancées (APTs). Nous avons découvert par le passé plusieurs attaques utilisant des logiciels malveillants tels que BlackEnergy qui avait entraîné une panne d'électricité. Mais dans l'opération **Groundbait**, l'attaque utilise des logiciels malveillants qui n'avaient encore jamais été utilisés. », explique Robert Lipovský, ESET Senior Malware Researcher.
Le vecteur d'infection principalement utilisé pour diffuser les logiciels malveillants dans l'opération Groundbait est le spear-phishing. «Au cours de nos recherches, nous avons observé un grand nombre d'échantillons ayant chacun son numéro de campagne ID désigné, avec un nom de fichier attrayant pour susciter l'intérêt de la cible. », explique Anton Cherepanov, Malware Researcher chez ESET.
L'opération a été nommée **Groundbait** (appât) par les chercheurs d'ESET suite à l'une des campagnes des cybercriminels. Alors que la majorité des autres campagnes utilisent les thèmes liés à la situation géopolitique actuelle de l'Ukraine et la guerre de Donbass pour attirer les victimes dans l'ouverture de la pièce jointe, la campagne en question, elle, affiche une liste de prix d'appâts de pêche à la place.
« Pour l'heure, nous ne sommes pas en mesure d'expliquer le choix de ce document comme leurre », ajoute Lipovský.
Comme c'est souvent le cas dans le monde de la cybercriminalité et des APTs, il est difficile de trouver la source de cette attaque. Nos recherches à ce sujet ont montré que les cybercriminels viennent très probablement de l'intérieur de l'Ukraine. Quoi qu'il en soit et au vu des cibles choisies, il est probable que cette opération de cyber-surveillance soit nourrie par une motivation politique. « En dehors de cela, toute nouvelle tentative d'attribution serait à ce point spéculatif. **Il est important de noter que, outre les séparatistes, les cibles de cette campagne sont les responsables gouvernementaux ukrainiens, les politiciens et les journalistes.** La possibilité de l'existence de fausses bannières doit également être prise en compte. », conclut Robert Lipovský.

Vous trouverez davantage de détails au sujet de l'opération Groundbait ici.

Article de Benoit Grunemwald
Directeur Commercial & Marketing ESET France

Réagissez à cet article

Source : *Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue*

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

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

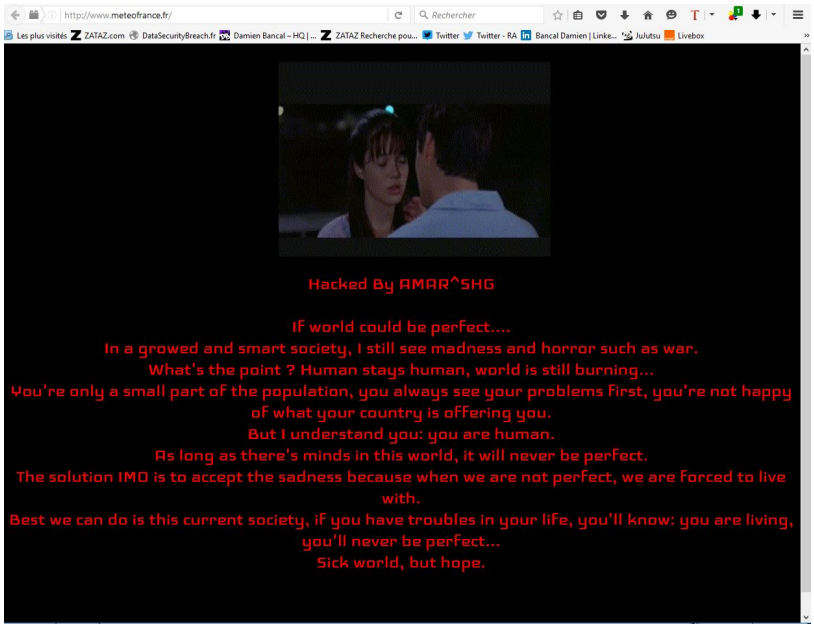
Réagissez à cet article

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

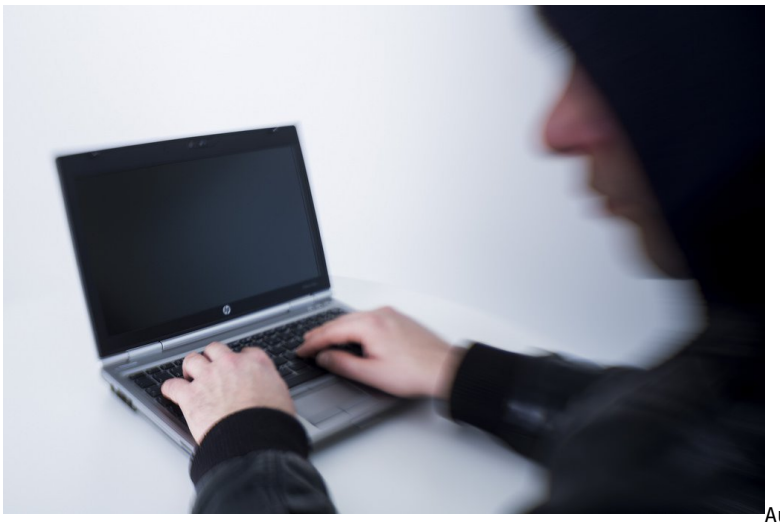
Source : *ZATAZ Détournement de DNS – Un pirate passe par Météo France – ZATAZ*

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*

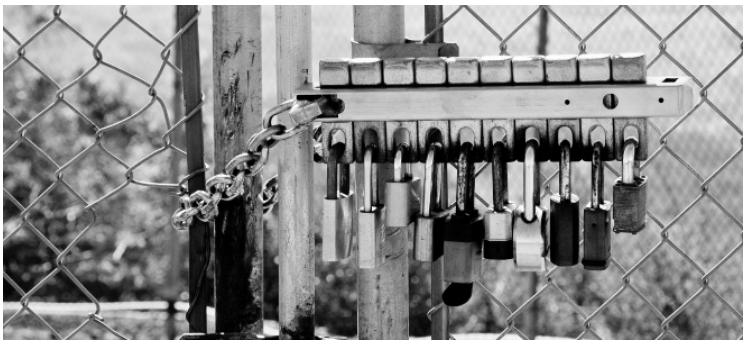
Auteur : David Pain

La sensibilisation des salariés à la Cybersécurité est essentielle

La sensibilisation des salariés à la Cybersécurité est essentielle

---

Bonne nouvelle : selon une étude menée par Solucom/Conscio Technologies et relayée par Les Échos, 82% des salariés sont sensibles aux risques informatiques et aux risques de vols d'informations. Mieux, 75% disent en avoir une bonne connaissance…. Des données intéressantes lorsque l'on sait que les failles de sécurité sont le plus souvent le fruit d'une négligence voire d'une malveillance humaine.



Une prise de conscience insuffisante ?

Si 88% des salariés disent être sensibilisés à l'enjeu de sécurité des mots de passe, dans les faits, ils ne sont que 47% à adopter les bonnes pratiques en la matière !
Parfois, les bonnes pratiques en elles-mêmes sont méconnues : 61% des salariés ne savent pas quoi faire à la réception d'un e-mail envoyé sous fausse identité, alors qu'ils sont 72% à se dire *sensibles* à la problématique.
On le voit, il y a un véritable enjeu pour les employeurs et les services IT : **mieux évangéliser, et ce de manière très concrète** pour que les salariés changent leurs comportements.

Quand implication et investissement vont de pair…

Un problème, donc, de communication en interne… Et, aussi, de moyens ? D'après une autre étude mentionnée par Les Échos, deux-tiers des responsables de service informatique considèrent que les budgets alloués par leur entreprise à la cybersécurité sont insuffisants.
=> L'étude, vue par Les Échos

Une formation infdispensable

Formation informatique cybercriminalité : Virus, arnaques et piratages informatiques, risques et solutions pour nos entreprises | Denis JACOPINI

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

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

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

Contactez-nous

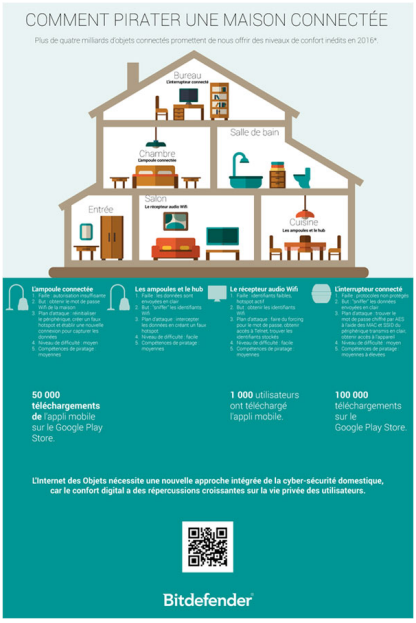
Réagissez à cet article

Source : *Cybersécurité : appuyez-vous sur vos salariés ! | Microsoft pour les PME*

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

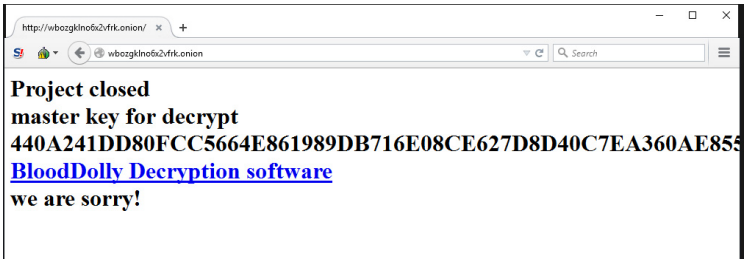
TelsaCrypt ? Voici finalement la clé de déchiffrement

	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*

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]

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 Edward Snowden déconseille Allo, la nouvelle messagerie de Google*

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 !*