Pokémon Go peut-il vraiment prendre le contrôle de votre compte Gmail ?

	Pokémon Go peut-il vraiment prendre le contrôle de votre compte Gmail ?

Malgré son succès indéniable, il semblerait que l'application Pokémon Go rencontre des premiers couacs, notamment en matière de protection de la vie privée. Selon certaines informations, depuis démenties, elle pourrait accéder et composer des emails sur le compte Gmail des utilisateurs.

Après avoir soulevé certains problèmes récemment avec le cas des voleurs armés aux États-Unis qui utilisaient le jeu pour cibler leurs victimes ou celui d'une jeune adolescente qui aurait retrouvé un cadavre pendant sa « chasse » aux Pokémon. La polémique n'en finit plus autour de Pokémon Go. C'est aujourd'hui un problème d'éthique et de sécurité qui est désormais pointé du doigt.

Pokémon Go : comment le jeu a rendu fou le monde entier

En effet lorsque vous installez et que vous jouez à Pokémon Go pour la première fois, le jeu sur smartphone développé par la firme Niantic, demande deux types de connexion. La première consiste à créer un compte via l'application tandis que la deuxième exige de se connecter directement depuis son compte Google. C'est la deuxième connexion qui soulève plusieurs problèmes.

Sur son blog, l'analyste en sécurité Adam Reeve expliquait ainsi ce week-end que cette identification par Google pouvait poser plusieurs problèmes puisque l'application accédait à plusieurs paramètres de votre compte Google : « Pokémon Go et Niantic peuvent désormais lire tous vos emails, envoyer des emails de votre part, accéder à vos documents Google Drive, rechercher dans votre historique de recherche et de navigation, accéder à toutes les photos privées hébergées sur Google Photos et bien davantage ». Des accès qui ne sont, bien évidemment, pas nécessaires pour profiter de l'expérience de jeu de l'application développée par Niantic.

Des informations démenties par Google et Niantic

Cependant, interrogé par le site Gizmodo, Adam Reeve a finalement fait marche arrière sur ses affirmations, expliquant ne pas être « certain à cent pour cent » que son billet de blog est exact. Il a par ailleurs expliqué au site Internet qu'il n'avait jamais développé lui-même d'application utilisant l'identification Google et n'a pas expérimenté ce qu'il indiquait sur son blog.

Du côté de Google également, l'information a été démentie auprès de Dan Guido, expert en sécurité informatique. La firme de Mountain View explique que les autorisations de Pokémon Go ne concernent que la partie « Mon Compte » de Google et n'autorise pas d'accès spécifique à différents services.

Enfin, le studio Niantic, qui développe l'application avec The Pokémon Company, a publié ce mardi un communiqué de presse afin de rassurer les utilisateurs : « Pokémon Go n'accède qu'aux informations basiques des profils Google (votre identification et votre adresse email). Aucune autre information de votre compte Google n'est ou ne sera collectée. […] Google réduira prochainement les autorisations de Pokémon Go uniquement aux données de profil dont Pokémon Go a besoin, les utilisateurs n'auront pas besoin d'effectuer le moindre changement ».

Article original de GEOFFROY HUSSON

Réagissez à cet article

Original de l’article mis en page : Pokémon Go peut-elle vraiment prendre contrôle de votre compte Gmail ?

Privacy Shield : un « bouclier » troué à refuser !

#Privacy Shield : un « bouclier » troué à refuser !

Le 8 juillet 2016, les États membres de l'Union européenne, réunis dans ce qu'on appelle le « comité de l'article 31 », se sont prononcé sur l'adoption de la décision d'adéquation qui encadrera les échanges de données personnelles entre les États-Unis et l'Union européenne : le Privacy Shield. Cette décision, adoptée dans la plus grande précipitation, ne répond pas aux inquiétudes exprimées ces dernières semaines à tour de rôle par le groupe des CNILs européennes, le Parlement européen et différents gouvernements européens, ainsi que par les associations de défense des droits.

Le 6 octobre 2015 la Cour de justice de l'Union européenne avait annulé l'accord du « Safe Harbor » couvrant les transferts de données depuis 2000, estimant que celui-ci permettait une collecte massive des données et une surveillance généralisée sans offrir de voies de recours effectives aux États-Unis pour les individus concernés en Europe. Aujourd'hui, force est de constater que le Privacy Shield ne répond pas non plus aux exigences de la Cour de justice.
Sur les principes de respect de la vie privée qui incombent aux entreprises couvertes par le Privacy Shield, on peut se demander l'utilité même d'une telle décision dans la mesure où celle-ci ne se substituera pas aux clauses contractuelles types ni aux règles internes d'entreprises, moins contraignantes et actuellement en vigueur, mais qu'elle s'y ajoutera. Cela signifie que si une entreprise couverte par le Privacy Shield s'en fait exclure pour non-respect des obligations qui lui incombent en matière de vie privée, elle pourra continuer à traiter des données avec les deux mécanismes internes cités plus hauts.
Mais le cœur de la décision se retrouve plutôt dans le chapitre sur l'accès aux données par les autorités publiques des États-Unis. Dans le texte, il n'est pas question de « surveillance de masse » mais plutôt de « collecte massive ». Or, si les États-Unis ne considèrent pas la collecte de masse comme de la surveillance, l'Union européenne, elle, par l'intermédiaire de sa Cour de justice, a tranché sur cette question en considérant, dans l'affaire C-362/14 Schrems c. Data Protection Commissioner, que la collecte massive effectuée par l'administration des États-Unis était de la surveillance de masse, contraire à la Charte des droits fondamentaux de l'Union européenne. Cette décision avait mené à l'invalidation du « Safe Harbor », et tout porte à croire que les voeux pieux et les faibles garanties d'amélioration exprimées par le gouvernement américain ne suffiront pas à rendre la décision du Privacy Shield adéquate avec la jurisprudence européenne.
Il en va de même sur la question des possibilités de recours. L'une des exigences de la CJUE, des CNIL européennes, du contrôleur des données personnelles et de la société civile était que toute personne concernée par un traitement de données avec cet État tiers puisse avoir la possibilité de déposer une plainte et de contester un traitement ou une surveillance illégale. Pour pallier cette sérieuse lacune du Safe Harbor, un mécanisme de médiateur (« #Ombudsperson ») a été instauré. L'initiative aurait été bonne si ce médiateur était réellement indépendant. Mais d'une part il est nommé par le Secrétaire d'État, d'autre part les requérants ne peuvent s'adresser directement à lui et devront passer par deux strates d'autorités, nationale puis européenne. L'Ombudsperson pourra simplement répondre à la personne plaignante qu'il a procédé aux vérifications, et pourra veiller à ce qu'une surveillance injustifiée cesse, mais le plaignant n'aura pas de regard sur la réalité de la surveillance. Cette procédure ressemble à celle mise en place en France par la loi Renseignement avec la #CNCTR et, pour les mêmes raisons, ne présente pas suffisamment de garanties de recours pour les citoyens.
Le projet de Privacy Shield, préparé et imposé dans la précipitation par la Commission européenne et le département du Commerce américain, ne présente pas les garanties suffisantes pour la protection de la vie privée des Européens. Il passe sciemment à côté du cœur de l'arrêt de la CJUE invalidant le Safe Harbor : la surveillance massive exercée via les collectes de données des utilisateurs. Les gouvernements européens et les autorités de protection des données doivent donc absolument refuser cet accord, et travailler à une réglementation qui protège réellement les droits fondamentaux. Les nécessités d'accord juridique pour les entreprises ayant fait de l'exploitation des données personnelles leur modèle économique ne peuvent servir de justification à une braderie sordide de la vie privée de dizaines de millions d'internautes européens.
Article original de La Quadrature du Net

Réagissez à cet article

Original de l'article mis en page : Privacy Shield : un « bouclier » troué à refuser ! – Global Security Mag Online

---

L'accord entre l'Europe et

les Etats-Unis sur les données personnelles sur le point d'être adopté

L'accord entre l'Europe et les Etats-Unis sur les données personnelles sur le point d'être adopté

Les Etats membres de lUE ont donné leur feu vert au «Privacy Shield», qui vient remplacer laccord «Safe Harbor» invalidé en octobre par la justice européenne.

Le «Privacy Shield» est sur la rampe de lancement. La Commission européenne l'a annoncé ce vendredi matin : le nouvel accord-cadre sur les transferts de données personnelles depuis le Vieux Continent vers les Etats-Unis a reçu le feu vert des Etats membres de l'Union, moins quatre abstentions (l'Autriche, la Slovénie, la Bulgarie et la Croatie, selon l'agence Reuters). Il devrait être adopté formellement par la Commission mardi prochain. Ce «bouclier de confidentialité» vient ainsi succéder à l'accord dit «Safe Harbor» (ou «sphère de sécurité»), invalidé il y a neuf mois par la justice européenne.

Deux ans de négociation

Mis en place en 2000, le Safe Harbor était censé garantir aux citoyens européens un niveau de protection suffisant de leurs données personnelles transférées sur le sol américain : les entreprises qui y adhéraient s'engageaient à respecter les normes de l'UE en la matière… via une certification annuelle qu'elles pouvaient s'autodécerner. Une «garantie» minimale qui a volé en éclats en 2013 avec les révélations d'Edward Snowden sur les pratiques de surveillance massive de la NSA, et notamment le programme Prism, qui permet à l'agence américaine d'accéder aux données stockées par les géants du Net.

Article original de Amaelle Guiton

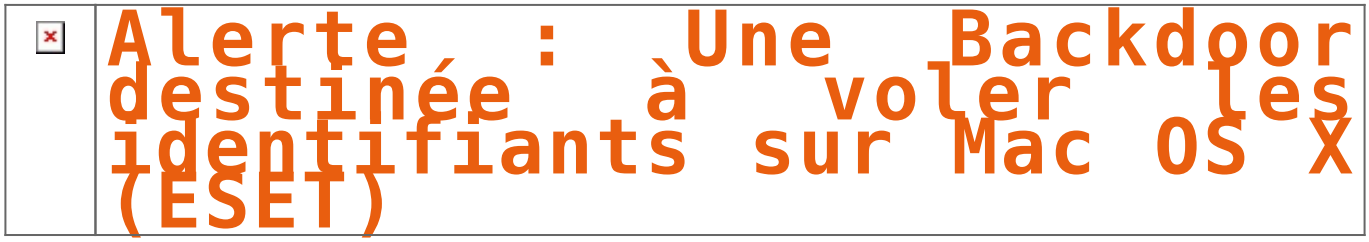
Photo Dado Ruvic. Reuters

Réagissez à cet article

Original de l’article mis en page : Données personnelles : laccord entre lEurope et les Etats-Unis sur le point dêtre adopté – Libération

---

Alerte : Une Backdoor destinée à voler les identifiants sur Mac OS X (ESET)



Le malware Keydnap exfiltre les mots de passe et les clés stockés dans le gestionnaire de mot de passe « KeyChain » de Mac OS X et crée une porte dérobée permanente.

Les chercheurs ESET se sont penchés sur OSX/Keydnap, un cheval de Troie qui vole les mots de passe et les clés stockées dans le gestionnaire de mot de passe « keychain », en créant une porte dérobée permanente.
Bien que la façon dont les victimes se trouvent exposées à cette menace ne soit pas très clair, nous pensons qu'elle pourrait se propager via des pièces jointes contenues dans les spams, des téléchargements à partir de sites non sécurisés ou d'autres vecteurs.
Le code malveillant Keydnap est distribué sous forme de fichier .zip avec le fichier exécutable imitant l'icône Finder habituellement appliqué aux fichiers texte ou JPEG. Cela augmente la probabilité que le destinataire double-clique sur le fichier. Une fois démarré, une fenêtre de terminal s'ouvre et la charge utile malveillante est exécutée.
À ce stade, la porte dérobée est configurée et le malware débute la collecte et l'exfiltration des informations de base figurant sur la machine Mac attaqué. À la demande de son serveur C&C, Keydnap peut obtenir les privilèges administratifs en ouvrant la fenêtre dédiée d'OS X.
Si la victime saisit ses identifiants, la porte dérobée fonctionne alors comme un root, avec le contenu exfiltré du porte-clés de la victime.
Bien qu'il existe des mécanismes de sécurité multiples en place au sein d'OS X pour réduire l'impact des logiciels malveillants, il est possible de tromper l'utilisateur.
Tous les utilisateurs d'OS X doivent rester vigilants car nous ne savons toujours pas comment Keydnap est distribué, ni combien de victimes ont été touchées », rapporte Marc-Etienne M. Léveillé, Malware Researcher chez ESET.
Des détails supplémentaires sur Keydnap peuvent être trouvés dans notre article technique disponible sur WeLiveSecurity.com.

Réagissez à cet article
Source : ESET

Le portable de Manuel Valls a-t-il été piraté par Israël ?

	Le portable de Manuel Valls a-t-il été piraté par Israël ?

Lors de son déplacement en Israël, une délégation de Matignon a laissé ses portables sans surveillance pendant une réception officielle. Et a relevé des anomalies de fonctionnement sur certains terminaux ensuite, assure l'Express.

Manuel Valls s'est-il fait pirater son smartphone lors de son déplacement en Israël, fin mai dernier ? C'est la question que posent nos confrères de l'Express. Lors de son déplacement qui avait pour ambition de relancer le processus de paix avec la Palestine, le Premier ministre, qui se présente volontiers comme « l'ami d'Israël » et la délégation l'accompagnant ont été priés de laisser leurs téléphones portables à l'accueil avant d'être reçu en haut lieu. Demande à laquelle ils auraient accédé, laissant leurs terminaux sans surveillance pendant l'entretien.
Problème : quand ils ont récupéré leurs terminaux pourtant sécurisés, certains présentaient des « anomalies », selon l'Express. Des dysfonctionnements qui peuvent laisser suspecter une tentative d'intrusion de la part des services secrets israéliens. L'Express ne précise pas le ou les modèles des terminaux concernés par ces tentatives d'espionnage supposées.

Pas d'espionnage entre alliés. Sans blague ?
Depuis, les téléphones en question ont été remis à l'Agence nationale de la sécurité des systèmes d'information (Anssi), qui mène l'enquête. Interrogée par nos confrères, celle-ci s'est toutefois refusée à tout commentaire. De son côté, Matignon reconnaît qu'un terminal est bien tombé en panne durant la visite du Premier ministre en Israël. Et indique à nos confrères qu'un allié n'espionne jamais ses amis. Défense de rire.
Rappelons que, pour les échanges les plus sensibles, les officiels français disposent de terminaux Teorem, fournis par Thales et habilités confidentiel-défense. Ceux-ci se révèlent toutefois peu pratiques d'usage, si bien que les ministres utilisent souvent des smartphones du commerce, durcis avec des technologies de sécurité complémentaires. Récemment, l'Elysée s'est ainsi équipé de smartphones Hoox, conçus par Bull. Ces machines, des smartphones Android bénéficiant d'une surcouche logicielle de sécurisation, sont vouées aux échanges de type « diffusion restreinte », un niveau de classification de l'information moins exigeant que le confidentiel-défense.
Article original de Reynald Fleychaux

Réagissez à cet article

Original de l'article mis en page : Le portable de Manuel Valls a-t-il été piraté par Israël ?

Cybersécurité : êtes-vous bien protégé?

	Cybersécurité : êtes-vous bien protégé?

De nos jours, impossible d'imaginer travailler dans le secteur des valeurs mobilières sans système informatique. Mais avec cet incontournable outil viennent plusieurs risques, qui peuvent faire un tort considérable aux conseillers et à leurs clients.

« Ces dommages peuvent nuire à la réputation d'un cabinet, l'exposer à des pertes financières et perturber gravement ses activités », prévient l'Association canadienne des courtiers de fonds mutuels (ACFM) dans un bulletin sur la cybersécurité publié la semaine dernière.

Selon des sondages réalisés aux États-Unis en 2011 et 2014 par le Financial Industry Regulatory Authority (FINRA), le secteur des valeurs mobilières est exposé à trois menaces de cybersécurité principales :

1. Les pirates informatiques qui infiltrent les systèmes d'une entreprise;
2. Les initiés qui compromettent les données d'un cabinet ou de ses clients;
3. Les risques opérationnels.

QUE FAIRE?

Pour se prémunir contre ces menaces, l'ACFM suggère à ses membres de se doter d'un cadre de cybersécurité, adapté à la taille de leur cabinet, en cinq étapes :

1. Identifier les biens qui doivent être protégés, de même que les menaces et les risques à leur égard;
2. Protéger ces biens à l'aide des mesures appropriées;
3. Détecter les intrusions et les infractions à la sécurité;
4. Intervenir s'il se produit un évènement de cybersécurité potentiel;
5. Évaluer l'incident et améliorer les mesures de sécurité à la lueur des évènements.

Pour mener à bien ce plan, l'ACFM propose de nombreuses pistes d'action que les cabinets peuvent suivre selon l'envergure de leurs activités.

Parmi elles, assurer la sécurité physique des lieux, notamment contre les menaces humaines, mais aussi environnementales, s'avère un incontournable, tout comme la mise en place de mesures de protection des systèmes (pare-feu récents, chiffrement des réseaux sans fil, processus de sauvegarde et de récupération, protocoles de mots de passe, etc.).

L'Association suggère également de se doter d'une procédure d'enquête sur le personnel, les sous-traitants et les fournisseurs, ainsi que d'instaurer une politique de cybersécurité et une formation continue obligatoire à ce sujet. Former une équipe d'intervention en cas d'incident peut aussi s'avérer une bonne idée.

Il importe de tester régulièrement la vulnérabilité des systèmes pour en détecter les failles et mieux les corriger. En cas d'incident, il est essentiel de le divulguer, rappelle l'ACFM, notamment au commissaire à la protection de la vie privée dans certains cas.

Finalement, il existe des assurances spécifiquement pour les menaces de cybersécurité.

Article original de conseiller.ca

Réagissez à cet article

Original de l’article mis en page : Cybersécurité : êtes-vous bien protégé? | Conseiller

---

Incroyable technique pour analyser les agissements des cybercriminels

	Incroyable technique pour analyser les agissements des cybercriminels

---

Depuis 2007, Zeus empoisonne la vie de millions d'internautes. Ce #logiciel malveillant s'installe sournoisement dans les ordinateurs afin de voler des informations bancaires. Zeus et ses variantes ont ainsi réussi à infecter les serveurs de grandes sociétés comme la NASA, Amazon et Facebook. Selon Mourad Debbabi, professeur et titulaire de la Chaire de recherche en sécurité des systèmes d'information à l'Université Concordia, la Toile est un véritable champ de bataille. Les attaques lancées par les pirates informatiques font des victimes chaque jour, mais les chercheurs ont ces cyberfraudeurs à l'œil : ils les observent pour mieux défendre les internautes, prévenir les fraudes et contre-attaquer !

L'équipe de Mourad Debbabi surveille notamment les « botnets » (contraction de *robot* et de *network*), des réseaux de machines infectées appelées « zombies » qui exécutent les directives des cybercriminels. Les gens installent des maliciels comme Zeus en cliquant sur une pièce jointe ou sur un lien compromis par un code nuisible. L'ordinateur contaminé envoie ensuite des courriels indésirables pour attirer d'autres victimes qui feront partie du *botnet*. Cet ensemble de machines infectées communique avec un ou des serveurs de commande et contrôle qui gèrent diverses attaques. Pour déjouer ces *botnets* et d'autres menaces, le professeur Debbabi et ses collaborateurs des paliers universitaire, gouvernemental et industriel canadiens ont développé une plateforme de cyber-renseignements. Il s'agit d'un réseau d'ordinateurs peu sécurisés qui « attirent » les cyberattaques, permettant aux chercheurs d'analyser en temps quasi réel une multitude de données (pourriels, virus, etc.) nécessaires pour contrecarrer les escrocs du Web. Cette cyberinformation sert à protéger le parc informatique et les renseignements privés des entreprises et des organisations : mise en quarantaine des ordinateurs infectés, pare-feu renforcé, logiciels de détection… Tel est pris qui croyait prendre !

Réagissez à cet article

Original de l’article mis en page : Cyberguerre : la science contrattaque | Scientifique en chef

---

Facebook vous suit à la trace pour vous suggérer des amis

	Facebook vous suit à la trace pour vous suggérer des amis

La géolocalisation de Facebook, utilisée notamment sur l'application mobile du réseau social, faisait déjà l'objet de nombreuses suspicions de la part des utilisateurs. Cette semaine, un porte-parole de Facebook a confirmé que la position géographique avait effectivement été utilisée par l'application pour suggérer de contacts que vous auriez pu croiser.

La fonction « Vous connaissez peut-être » de Facebook est souvent surprenante par sa précision, suggérant généralement des contacts pertinents. Si le site n'a jamais révélé vraiment les méthodes utilisées pour faire mouche aussi souvent, un de ses secrets vient en revanche d'être découvert : la géolocalisation permettrait de déterminer les personnes que vous fréquentez et qui disposent d'un compte. Concrètement, si deux personnes disposant d'un compte Facebook se trouvent au même endroit et ont activé la géolocalisation, le site proposera alors de les mettre en relation sur le réseau social.

« La localisation elle-même ne suffit pas à déterminer que deux personnes peuvent être amies », indique un porte-parole de Facebook au journal anglais The Telegraph. Et c'est justement un des arguments avancés par les détracteurs de cette fonction, qui y voient une atteinte à la vie privée. Le site n'étant pas capable de déterminer si deux personnes se trouvant au même endroit sont amies, ou même si elles se connaissent réellement, l'usage d'une telle fonction peut sembler abusif sur certains aspects, et poser quelques problèmes concernant l'anonymat que certains voudraient conserver en public. Facebook a cependant indiqué que cette fonction n'était aujourd'hui plus active sur son application mobile, et que celle-ci avait simplement fait l'objet d'un test limité. Les plus inquiets peuvent néanmoins désactiver la géolocalisation pour l'application.

Article original de Nicolas AGUILA

Réagissez à cet article

Original de l'article mis en page : Facebook vous suit à la trace pour vous suggérer des amis

Inquiétantes intrusions dans les réseaux d’entreprises

	Inquiétantes intrusions dans les réseaux d’entreprises

Les intrusions dans les réseaux informatiques des entreprises se sont multipliées en France ces derniers mois et labsence de vols de données laisse craindre des tentatives de sabotages ou dattaques terroristes, a déclaré lundi le directeur général de lAgence nationale de la sécurité des systèmes dinformation (Anssi).

Le Secrétariat général de la défense et la sécurité nationale (SGDSN) et l'Anssi, deux services rattachés à Matignon, ont présenté lundi les trois premiers arrêtés liés à la protection des opérateurs d'importance vitale dans la santé, la gestion de l'eau et l'alimentation, qui entreront en vigueur le 1er juillet.

« Il y a de plus en plus d'attaquants, ce sont des agents dormants qui préparent les choses », a expliqué Guillaume Poupard à des journalistes. « Il y a eu beaucoup de cas à traiter ces derniers mois ».

Ces intrusions, par exemple par le biais d'emails piégés envoyés dans les entreprises, permettent aux attaquants de cartographier un réseau en toute discrétion et, en passant d'un réseau à l'autre, de pénétrer dans des zones inattendues.

« Ils prennent pied progressivement (..) et on les retrouve très profond au sein des réseaux d'entreprises, à des endroits où il n'y a même plus d'informations secrètes à voler, par exemple sur les systèmes de production de contrôle qualité », a ajouté Guillaume Poupard.

Ce nouveau type d'intrusion est d'autant plus inquiétant qu'il est presque plus facile d'entrer dans un réseau pour en modifier le fonctionnement ou en prendre le contrôle que pour voler des données, a-t-il souligné.

Au contraire de la banque, de l'aérospatiale et de l'automobile, habitués à surveiller de près leurs réseaux, l'industrie est encore mal préparée, étant moins sujette aux vols de données, a noté Guillaume Poupard.

« L'idée que des gens qui depuis l'autre bout du monde puissent chercher à détruire leur système de production c'est un nouveau scénario qui n'a pas vraiment d'équivalent dans le monde réel », a-t-il souligné.

Pour mieux défendre les PME, « un des maillons faibles », cible rêvée d'un attaquant, il prône le recours aux solutions de « cloud computing » des spécialistes de la sécurité numérique et à l'intégration de systèmes de protection dans les machines outils et les automates industriels dès leur conception. (Cyril Altmeyer, édité par Jean-Michel Bélot)

Réagissez à cet article

Original de l'article mis en page : SAFRAN : France : Inquiétantes intrusions dans les réseaux dentreprises

Des caméras de surveillance piratées pour mener des attaques DDoS

	Des caméras de surveillance piratées pour mener des attaques DDoS

Tous ceux qui refusent d'admettre que l'Internet des Objets pourrait être à l'origine de nombreuses menaces dans la sphère informatique de demain vont probablement avoir du mal à tenir leur position après l'affaire présentée ici. En effet, des hackers ont utilisé un réseau de 25 000 caméras de surveillance piratées pour conduire des attaques DDoS.

Des caméras de surveillance piratées pour former un botnet

Il y a quelques heures, l'entreprise Sucuri, spécialisée dans la sécurité informatique, a découvert que des hackers avaient réussi à prendre le contrôle de quelques 25 000 caméras de surveillance présentes au quatre coins de la planète.

Mais l'objectif des pirates n'était pas que de récupérer des images ou d'espionner des individus puisqu'ils ont utilisé les caméras de surveillance pour créer un botnet, autrement dit un réseau de machines contrôlées à distance par un seul et même individu.

Capables d'agir ensemble, les 25 000 caméras ont ainsi pu être à l'origine d'attaques DDoS contre plusieurs sites Internet. En effet, les hackers se sont servis du réseau de caméras de surveillance pour envoyer des requêtes simultanées sur des sites causant ainsi leur paralysie pendant de longues minutes.

Une preuve supplémentaire de la menace que laissent planer les objets connectés

Si l'utilisation d'objets connectés par les pirates pour mener des attaques DDoS est tout sauf une nouveauté, c'est l'ampleur de l'attaque qui surprend. En effet, même les spécialistes sont restés « coi » devant la capacité d'un réseau de 25 000 caméras de surveillance à générer autant de requêtes simultanément.

L'autre surprise tient au fait que les caméras piratées sont dispatchées aux quatre coins de la planète. 2% seraient d'ailleurs basées en France alors que c'est aux Etats-Unis, en Indonésie et à Taïwan que la majorité d'entre elles se situerait.

Sucuri a d'ailleurs cherché à comprendre ce que pouvait avoir en commun l'ensemble de ces appareils et la piste la plus sérieuse mène à BustyBox, un système qui serait intégré à tous. Or, une importante faille avait été découverte au printemps dans celui-ci ce qui aurait pu permettre à des pirates de l'exploiter pour commettre leurs actions.

Affaire à suivre…

Article original de Jérôme DAJOUX

Réagissez à cet article

Original de l'article mis en page : Des caméras de surveillance piratées pour mener des attaques DDoS