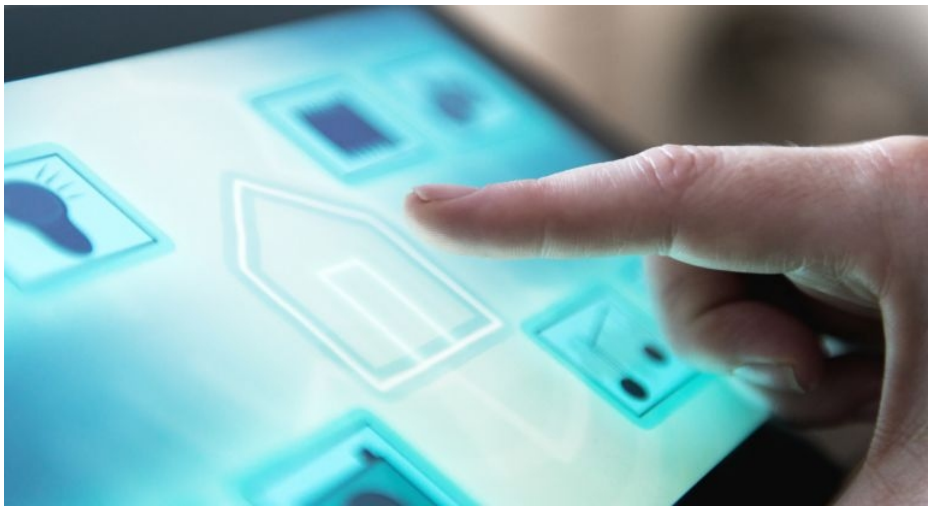
Jusqu’où les Objets connectés sont les maillons faibles de la cybersécurité ?

	Jusqu’où les Objets connectés sont les maillons faibles de la cybersécurité ?

La Chine s'impose parmi les principaux pays créateurs d'objets quotidiens connectés à l'internet, mais elle génère ainsi de gigantesques failles sécuritaires exploitables par des pirates informatiques, a prévenu mardi John McAfee, créateur américain du logiciel antivirus portant son nom.

S'exprimant devant une conférence spécialisée à Pékin, M. McAfee a cité des précédents, dans lesquels des pirates sont parvenus à distance à prendre le contrôle de coffre-forts, de systèmes de chauffage, mais aussi d'ordinateurs de bord d'automobiles ou d'aéroplanes.

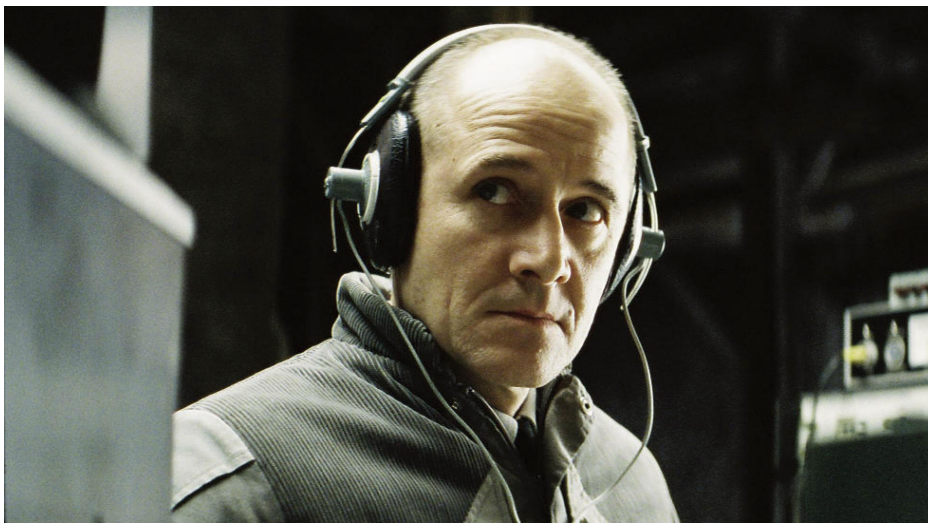
« La Chine prend la tête des progrès sur les objets intelligents, depuis les réfrigérateurs jusqu'aux thermostats, et c'est le maillon faible de la cybersécurité », a-t-il martelé, disant vouloir « lever un drapeau rouge » d'avertissement.
« Il y a tellement plus de ces objets, et plus vous en connectez ensemble, plus les risques de piratage augmentent », a encore souligné John McAfee.
L'excentrique septuagénaire avait fait fortune aux débuts d'internet dans les années 1990, après avoir mis au point un logiciel antivirus qui porte son nom et est maintenant la propriété d'Intel.
Plombé par la crise financière de 2008, il avait défrayé la chronique en 2012 après la mort de son voisin au Belize, pays où il vivait à l'époque et qu'il avait fui après l'ouverture d'une enquête de la police locale.
M. McAfee a livré à Pékin un discours au ton sombre et inquiétant, à l'heure où sa nouvelle société MGT Capital se prépare à lancer de nouveaux produits de cybersécurité d'ici la fin de l'année.
« Notre espèce n'a jamais été confrontée jusqu'ici à une menace de cette ampleur. Et pour l'essentiel, nous n'en prenons pas conscience », a-t-il averti.
« Vous pouvez penser que j'exagère, que je tombe dans l'alarmisme. Mais je compte parmi mes amis beaucoup de +hackers+ (pirates) qui ont les capacités de faire d'énormes dégâts si l'envie leur en prend », a-t-il ajouté.
A l'instar de Xiaomi, fabricant de smartphones ayant élargi son offre dans l'électroménager « intelligent », nombre d'entreprises chinoises intègrent désormais une connexion wi-fi à des produits variés, des autocuiseurs pour riz aux purificateurs d'air, permettant aux usagers de les allumer à distance depuis leur téléphone.
De telles connexions créent de graves failles qui accentuent les vulnérabilités de leurs réseaux, selon John McAfee.
Dans un entretien avec des journalistes à Pékin, l'Américain a cependant noté « n'avoir entendu parler d'aucune » attaque informatique de grande ampleur en Chine sur l'année passée, tandis que les Etats-Unis en enregistraient « des centaines ».

Original de l'article mis en page : Objets connectés : le créateur de l'antivirus McAfee met en garde la Chine contre les failles de sécurité | La Provence

---

Collectes massives et illégales par le

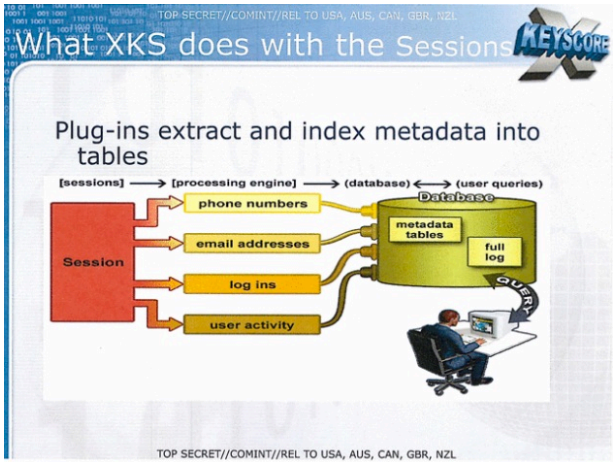
Renseignement allemand



Collectes massives et illégales par le Renseignement allemand

Après avoir réalisé un contrôle sur place des services de renseignement, la Cnil allemande a dressé un bilan extrêmement critique des activités du Bundesnachrichtendienst (BND) en matière de collecte d'informations sur Internet.

Le site Netzpolitik a dévoilé le contenu d'un rapport jusque là confidentiel produit en juillet 2015 par Andrea Voßhoff, le commissaire à la protection des données en Allemagne, qui accable les services de renseignement allemands. Le rapport a été réalisé après la visite de l'homologue de la Cnil dans la station d'écoutes Bad Aibling, opérée conjointement en Bavière par l'agence allemande du renseignement, la Bundesnachrichtendienst (BND), et par la National Security Agency (NSA) américaine.
Malgré les difficultés à enquêter qu'il dénonce, Voßhoff dénombre dans son rapport 18 violations graves de la législation, et formule 12 réclamations formelles, qui obligent l'administration à répondre. Dans un pays encore meurtri par les souvenirs de la Stasi, le constat est violent.
L'institution reproche au BND d'avoir créé sept bases de données rassemblant des informations personnelles sur des suspects ou simples citoyens lambda, sans aucun mandat législatif pour ce faire, et de les avoir utilisées depuis plusieurs années au mépris total des principes de légalité. Le commissaire a exigé que ces bases de données soient détruites et rendues inutilisables.



Parmi elles figure une base assise sur le programme XKeyScore de la NSA, qui permet de réunir et fouiller l'ensemble des informations collectées sur le Web (visibles ou obtenues par interception du trafic), pour les rendre accessibles aux analystes qui veulent tout savoir d'un individu et de ses activités en ligne. Alors que XKeyScore est censé cibler des suspects, Voßhoff note que le programme collecte « un grand nombre de données personnelles de personnes irréprochables », et cite en exemple un cas qu'il a pu consulter, où « pour une personne ciblée, les données personnelles de quinze personnes irréprochables étaient collectées et stockées », sans aucun besoin pour l'enquête…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Le Renseignement allemand pris en flagrant délit de collectes massives illégales – Politique – Numerama

Ce que Facebook sait (espionne) sur vous

	Ce que Facebook sait (espionne) sur vous

Si vous vous êtes déjà demandé pourquoi Facebook semble connaître une quantité alarmante de chose sur vous; comme tous les sites Web que vous visitez, pour qui vous votez, et quelle quantité vous buvez, voici pourquoi.

Où que vous alliez, quoi que vous fassiez (si c'est en ligne) les chances sont que Mark Zuckerberg vous observe, et apprend.
Facebook recueille des données lorsque vous êtes sur d'autres sites, dans les applications, et dans Facebook lui-même; développant un profil de 98 *« points de données »* sur vous.
Facebook a récemment déployé une mise à jour de son outil Ad Préférences qui révèle un peu plus les données recueillies par Facebook (tout est fait pour vous servir des publicités *« personnalisées »*).
Certaines d'entre elles sont assez alarmantes (comme si vous êtes enceinte, votre race, et votre titre d'emploi) toutes ces données sont récoltées tranquillement, sans avoir un formulaire à remplir.
Voici les 98 *« points de données »* que Facebook sait probablement de vous, où s'il ne les connait pas encore, il essaye de les apprendre, selon le Washington Post.

Qu'est-ce que Facebook sait sur vous

1. L'emplacement
2. L'âge
3. La génération
4. Le sexe
5. La langue
6. Le niveau d'éducation
7. Le domaine d'études
8. L'école
9. L'affinité ethnique
10. Le revenu et la valeur nette
11. La valeur de la propriété et le type
12. La valeur domestique
13. La surface du terrain
14. La superficie de la maison
15. L'année de construction de la maison
16. La composition du ménage
17. Les utilisateurs qui ont un anniversaire dans les 30 jours
18. Les utilisateurs qui sont loin de leur famille ou de leur ville natale
19. Les utilisateurs qui sont amis avec quelqu'un qui a un anniversaire, nouvellement marié ou engagé, récemment déménagé, ou a un anniversaire à venir
20. Les utilisateurs dans les relations à longue distance
21. Les utilisateurs qui ont de nouvelles relations
22. Les utilisateurs qui ont de nouveaux emplois
23. Les utilisateurs qui sont nouvellement engagés
24. Les utilisateurs qui sont nouvellement mariés
25. Les utilisateurs qui ont récemment déménagé
26. Les utilisateurs qui ont des anniversaires bientôt
27. Les parents
28. Les futurs parents
29. Les occupations, rangées par « type » (football, mode, etc.)
30. Les utilisateurs qui sont susceptibles de participer à la politique
31. Les conservateurs et les libéraux
32. La situation amoureuse
33. L'employeur
34. Le travail
35. Les fonctions du travail
36. Les statuts au travail
37. Les loisirs
38. Les utilisateurs qui possèdent des motos
39. Les utilisateurs qui ont l'intention d'acheter une voiture (et quel type / marque de voiture, et dans combien de temps)
40. Les utilisateurs qui ont acheté des pièces ou accessoires automobiles récemment
41. Les utilisateurs qui sont susceptibles d'avoir besoin de pièces ou de services automobiles
42. Le style et la marque de voiture que vous conduisez
43. L'année d'achat de votre voiture
44. L'âge de votre voiture
45. Combien d'argent l'utilisateur est susceptible de dépenser pour la voiture suivante
46. Lorsque l'utilisateur est susceptible d'acheter la voiture suivante
47. Combien d'employés possède votre entreprise
48. Les utilisateurs qui possèdent des petites entreprises
49. Les utilisateurs qui travaillent dans la gestion ou qui sont cadres
50. Les utilisateurs qui ont fait don à la charité (divisés par type)
51. Le système d'exploitation
52. Les utilisateurs qui jouent à des jeux de navigateur
53. Les utilisateurs qui possèdent une console de jeu
54. Les utilisateurs qui ont créé un événement sur Facebook
55. Les utilisateurs qui ont utilisé les paiements Facebook
56. Les utilisateurs qui ont passé plus que la moyenne sur les paiements Facebook
57. Les utilisateurs qui administrent une page Facebook
58. Les utilisateurs qui ont récemment téléchargé des photos sur Facebook
59. Le navigateur Internet
60. Le service de messagerie e-mail
61. Le passage précoce / tardif à la technologie
62. Les expatriés (divisés par le pays d'origine)
63. Les utilisateurs qui appartiennent à une coopérative de crédit, la banque nationale ou banque régionale
64. Les utilisateurs qui sont investisseurs (divisés par type d'investissement)
65. Le nombre de crédits
66. Les utilisateurs qui utilisent des cartes de crédit
67. Le type de carte
68. Les utilisateurs qui ont une carte de débit
69. Les utilisateurs qui effectuent un solde sur leur carte de crédit
70. Les utilisateurs qui écoutent la radio
71. La préférence dans les émissions télévisées
72. Les utilisateurs qui utilisent un appareil mobile (divisé par quelle marque ils utilisent)
73. Le type de connexion Internet
74. Les utilisateurs qui ont récemment fait l'acquisition d'un smartphone ou d'une tablette
75. Les utilisateurs qui accèdent à Internet via un smartphone ou une tablette
76. Les utilisateurs qui utilisent des coupons
77. Les types de vêtements achetés
78. Le temps passé dans les magasins
79. Les utilisateurs qui sont des « gros » acheteurs de bière, de vin ou de spiritueux
80. Les utilisateurs qui achètent dans les épiceries (et quelles types)
81. Les utilisateurs qui achètent des produits de beauté
82. Les utilisateurs qui achètent des médicaments contre les allergies, la toux / médicaments contre le rhume, les produits de soulagement de la douleur
83. Les utilisateurs qui dépensent de l'argent sur les produits ménagers
84. Les utilisateurs qui dépensent de l'argent sur les produits pour les enfants ou les animaux domestiques, et quels types d'animaux de compagnie
85. Les utilisateurs dont les ménages font des achats plus que ce qui est en moyenne
86. Les utilisateurs qui ont tendance à faire des achats en ligne
87. Les types de restaurants
88. Les types de boutiques et magasins
89. Les utilisateurs qui sont « réceptifs » aux offres des compagnies offrant des assurances auto en ligne, l'éducation ou des prêts hypothécaires plus élevés, les cartes prépayées / la TV par satellite
90. La durée du temps passé dans une maison
91. Les utilisateurs qui sont susceptibles de se déplacer rapidement
92. Les utilisateurs qui sont intéressés par les Jeux Olympiques, le football, le cricket ou le Ramadan
93. Les utilisateurs qui voyagent fréquemment, pour le travail ou pour le plaisir
94. Les utilisateurs qui font la navette jusqu'au travail
95. Les types de vacances d'un utilisateur
96. Les utilisateurs qui sont récemment revenus d'un voyage
97. Les utilisateurs qui ont récemment utilisé une application de voyage
98. Les utilisateurs qui participent à une multipropriété

Source : **Metro.co.uk**

Réagissez à cet article

Original de l’article mis en page : Voici 98 choses que Facebook sait sur vous

---

Retrouver l’auteur d’un E-mail à partir de l’adresse IP : Le demandeur condamné

Retrouver l’auteur d’un E-mail à partir de l’adresse IP : Le demandeur condamné

Le TGI de Meaux a débouté l'entreprise qui voulait obtenir de Numericable les noms, prénoms, adresses et coordonnées complètes de l'auteur d'un email frauduleux à partir de son adresse IP.

Dans une ordonnance de référé du 10 août 2016 repérée par Legalis, le tribunal de grande instance de Meaux (Seine-et-Marne) a débouté l'entreprise qui voulait obtenir de Numericable les données d'identification correspondant à l'adresse IP de l'auteur présumé d'un email frauduleux.
Comment en est-on arrivé là ? En début d'année, la société France Sécurité a préparé une proposition commerciale à l'attention d'Airbus Helicopters dans le cadre d'un appel d'offres. Dans la foulée, le distributeur d'équipements de protection individuelle a reçu un courriel d'un individu se faisant passer pour un employé d'Airbus et lui demandant de transmettre par courriel le fichier contenant la proposition… Suspectant la fraude, France Sécurité a contacté Airbus. Le nom associé au courriel était bien celui d'un de ses employés, mais il n'était pas l'auteur des courriels en question.

Usurpation d'identité
Dans un premier temps, une plainte a été déposée contre X pour usurpation d'identité. Parallèlement, le département informatique de France Sécurité a identifié l'adresse IP de l'expéditeur du courriel (transmis via Gmail) ainsi que le FAI hôte, à savoir : Numericable. Un procès-verbal de constat d'huissier a été établi. Ensuite, le 28 juin 2016, France Sécurité a déposé plainte auprès du procureur de la République près le tribunal de grande instance de Nantes. Et le 8 juillet 2016, l'entreprise a fait assigner devant le juge des référés du TGI de Meaux le câblo-opérateur. Le but : obtenir du tribunal qu'il ordonne au FAI de communiquer dans un délai de 48 heures les données d'identification correspondant à l'adresse IP en cause. Car, selon le demandeur, le câblo-opérateur est tenu de conserver les données permettant l'identification de son client et de déférer aux demandes de l'autorité judiciaire. Et ce en application de la loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004. France Sécurité souhaitait également qu'une astreinte soit versée par Numericable en cas de dépassement de ce délai, en plus des frais irrépétibles… Sans succès.

L'adresse IP, une donnée personnelle
Le juge est parti du principe que l'adresse IP est une donnée à caractère personnel. Par ailleurs, il a considéré que la collecte de cette donnée constitue un traitement au sens de la loi informatique et libertés. Une telle collecte aurait donc dû faire l'objet d'une autorisation de la Commission nationale informatique et libertés (Cnil) accordée à France Sécurité. Cela n'a pas été le cas. Par ailleurs, le juge considère que le cadre juridique applicable dans ce dossier ne peut pas être celui de la LCEN de 2004. Selon lui, Numericable n'est pas visé en tant que « personne dont l'activité est d'offrir un accès à des services de communication au public » en relation avec « la création d'un contenu » en ligne.
Résultat : le TGI de Meaux a débouté France Sécurité de toutes ses demandes. L'entreprise a été condamnée aux entiers dépens et au versement de 2 000 euros au titre des frais irrépétibles…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : IP : Numericable n’a pas à communiquer les données d’identification

---

Position du CERT-FR (Computer Emergency Response Team de l’ANSSI) vis à vis de Pokemon Go

Position du CERT-FR (Computer Emergency Response Team de l’ANSSI) vis à vis de Pokemon Go

---

Cyber-risques liés à l'installation et l'usage de l'application Pokémon GoLancé courant juillet par la société Niantic, le jeu Pokémon Go est depuis devenu un phénomène de société, au point d'être installé sur plus de 75 millions de terminaux mobiles dans le monde. Certains acteurs malveillants ont rapidement tenté d'exploiter la popularité du jeu à des fins criminelles. Certaines précautions s'imposent donc avant de pouvoir tenter de capturer un Dracaufeu ou un Lippoutou sans porter atteinte à la sécurité de son ordiphone.

Cyber-risques liés à l'installation et l'usage de l'application Pokémon Go

Lancé courant juillet par la société Niantic, le jeu Pokémon Go est depuis devenu un phénomène de société, au point d'être installé sur plus de 75 millions de terminaux mobiles dans le monde. Certains acteurs malveillants ont rapidement tenté d'exploiter la popularité du jeu à des fins criminelles. Certaines précautions s'imposent donc avant de pouvoir tenter de capturer un Dracaufeu ou un Lippoutou sans porter atteinte à la sécurité de son ordiphone.

Applications malveillantes

Des sociétés spécialisées en sécurité informatique ont mis en évidence la présence de nombreuses fausses applications se faisant passer pour une version officielle du jeu. Ces applications sont susceptibles de naviguer sur des sites pornographiques pour simuler des clics sur des bannières publicitaires, de bloquer l'accès au terminal et de ne le libérer qu'en contrepartie d'une rançon, ou bien même d'installer d'autres codes malveillants. Au vu du nombre d'applications concernées (plus de 215 au 15 juillet 2016), cette technique semble très populaire, en particulier dans les pays où le jeu n'est pas encore disponible via les sites officiels.

Niveau de permissions demandées par l'application

La version initiale du jeu sur iOS présentait un problème au niveau de la gestion des permissions. En effet, le processus d'enregistrement d'un compte Pokemon Go à l'aide d'un compte Google exigeait un accès complet au profil Google de l'utilisateur.
Suite à la prise de conscience de ce problème, la société Niantic a rapidement réagi en précisant qu'il s'agissait d'une erreur lors du développement. Elle propose désormais une mise à jour pour limiter le niveau d'accès requis au profil Google de l'utilisateur. A noter que la version Android du jeu ne semble pas avoir été affectée par ce problème.
Dans le doute, il est toujours possible de révoquer cet accès en se rendant sur la page de gestion des applications autorisées à accéder à son compte Google.

Collecte de données personnelles

De par son fonctionnement, l'application collecte en permanence de nombreuses données personnelles qui sont ensuite transmises au développeur du jeu, par exemple les informations d'identité liées au compte Google ou la position du joueur obtenue par GPS. Certaines indications visuelles (nom de rue, panneaux, etc) présentes sur les photos prises avec l'application peuvent aussi fournir des indications sur la position actuelle du joueur. La désactivation du mode « réalité augmentée » lors de la phase de capture permet de se prémunir de ce type de risques (et accessoirement, de réduire l'utilisation de la batterie de l'ordiphone).

Pokemons et BYOD

Il peut être tentant d'utiliser un ordiphone professionnel pour augmenter les chances de capture d'un Ronflex. Même s'il est souvent délicat de répondre par la négative à une requête émanant d'un VIP, il semble peu opportun de déployer ce type d'application dans un environnement professionnel, en raison des différents risques évoqués précédemment.

Recommandations

Le CERT-FR recommande de n'installer que la version originale du jeu présente sur les boutiques d'Apple et de Google. En complément, il convient de désactiver la possibilité d'installer une application téléchargée depuis un site tiers (sous Android, paramètre « Sources inconnues » du menu « Sécurité »).
Il est également conseillé de vérifier les permissions demandées par l'application. La version originale du jeu nécessite uniquement :
• d'accéder à l'appareil photo pour les fonctionnalités de réalité augmentée ;
• de rechercher des comptes déjà présents sur l'appareil ;
• de localiser l'utilisateur grâce au GPS ou aux points d'accès Wi-Fi ;
• d'enregistrer localement des fichiers sur le téléphone.
Toute autre permission peut sembler suspecte et mettre en évidence la présence sur l'ordiphone d'une version altérée de l'application.
Le CERT-FR suggère de mettre en place un cloisonnement entre l'identité réelle du joueur et celle de dresseur Pokémon. Pour cela, il est possible d'ouvrir un compte directement auprès du Club des dresseurs Pokémon [8] ou bien de créer une adresse Gmail dédiée à cet usage.
Enfin, le CERT-FR déconseille de pratiquer cette activité dans des lieux où le geo-tagging du joueur pourrait avoir des conséquences (lieu de travail, sites sensibles, etc) [9]…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Bulletin d'actualité CERTFR-2016-ACT-031

Déchiffrement des

communication numériques (Telegram et autres). Où en est-on ?

Déchiffrement des communication numériques (Telegram et autres). Où en est-on ?

Ce mardi 23 Août, Bernard Cazeneuve se réunissait avec son homologue allemand pour discuter d'une initiative européenne contre le chiffrement des données, afin de lutter contre le terrorisme. Une initiative qui ne fait pas l'unanimité.

Une initiative européenne contre les chiffrements trop forts ?

Face au terrorisme international et sachant que les messageries instantanées visées par le projet de loi sont majoritairement américaines, Bernard Cazeneuve s'en remet à une initiative européenne. L'idée serait d'étendre aux services de messageries et d'appels sur internet, les mêmes règles de sécurité et de confidentialité destinées jusque-là, aux opérateurs télécom. Le ministre a ainsi fermement déclaré vouloir obliger les services en ligne «*non coopératifs*» à «*retirer des contenus illicites ou déchiffrer des messages dans le cadre d'enquêtes judiciaires, que leur siège soit en Europe ou non*».

Conscient de la polémique qui entoure ce projet de loi, le ministre a précisé que l'utilisation des données déchiffrées ne servirait que dans le cadre « *judiciaire* ». Ce qui voudrait dire qu'elles ne seraient pas utilisées par les services secrets, comme le redoutent beaucoup de personnes. Se voulant rassurant, il a insisté « *Il n'a bien sûr, jamais été question de remettre en cause le principe du chiffrement des échanges* ». Le 16 septembre prochain, le projet de loi contre le chiffrement des données sera discuté lors du sommet des chefs d'états européens.

…[lire la suite]

Original de l'article mis en page : Une initiative franco-allemande contre le chiffrement numérique

Révélations sur de petits piratages informatiques entre alliés…

Révélations sur de petits piratages informatiques entre alliés…

C’est une révélation assez rare pour être soulignée, mais elle était passée inaperçue. Bernard Barbier, l’ancien directeur technique de la DGSE, le service de renseignement extérieur français, s’est livré en juin dernier à une longue confession devant les élèves de l’école d’ingénieurs Centrale-Supélec (voir vidéo ci-dessous), comme l’explique Le Monde.

Cet ex-cadre de l’espionnage a notamment confirmé que les Etats-Unis étaient bien responsables de l’attaque informatique de l’Elysée en 2012.

Entre les deux tours de la présidentielle de 2012, des ordinateurs de collaborateurs de Nicolas Sarkozy avaient été infectés à l’Elysée. Jusqu’à présent, les soupçons se portaient bien vers la NSA mais ils n’avaient jamais été confirmés. « Le responsable de la sécurité informatique de l’Elysée était un ancien de ma direction à la DGSE. Il nous a demandé de l’aide. On a vu qu’il y avait un malware », a expliqué Bernard Barbier en juin dernier. « En 2012, nous avions davantage de moyens et de puissance techniques pour travailler sur les métadonnées. J’en suis venu à la conclusion que cela ne pouvait être que les Etats-Unis. »

La France aussi impliquée dans un pirate informatique

Ce cadre de la DGSE a ensuite été envoyé par François Hollande pour s’entretenir avec ses homologues américains. « Ce fut vraiment un grand moment de ma carrière professionnelle », explique-t-il. « On était sûrs que c’était eux. A la fin de la réunion, Keith Alexander (l’ex-directeur de la NSA), n’était pas content. Alors que nous étions dans le bus, il me dit qu’il est déçu, car il pensait que jamais on ne les détecterait. Et il ajoute : ‘Vous êtes quand même bons.’ Les grands alliés, on ne les espionnait pas. Le fait que les Américains cassent cette règle, ça a été un choc. »

Pourtant, au cours de cette conférence, Bernard Barbier a aussi révélé l’implication de la France dans une vaste opération d’espionnage informatique commencée en 2009 qui avait touché notamment l’Espagne, la Grèce ou l’Algérie. Le Canada, lui aussi visé, avait à l’époque soupçonné Paris, mais rien n’avait été confirmé en France. « Les Canadiens ont fait du reverse sur un malware qu’ils avaient détecté. Ils ont retrouvé le programmeur qui avait surnommé son malware Babar et avait signé Titi. Ils en ont conclu qu’il était français. Et effectivement, c’était un Français. »

Article original de Thomas Liabot

Réagissez à cet article

Original de l’article mis en page : Les Etats-Unis étaient bien à l’origine du piratage informatique de l’Elysée en 2012 – leJDD.fr

---

Le logiciel de téléchargement Transmission à nouveau piraté

Le logiciel de téléchargement Transmission à nouveau piraté

Le Net Expert vous avait déjà informé en juillet dernier de cet type d'attaque dont avait été victime la sphère Apple. Apparemment la leçon n'a pas servi. Même méthode, même punition.

Pour la deuxième fois en moins de six mois, la version Mac du logiciel Transmission a été corrompue, a révélé mardi 30 août l'entreprise de sécurité informatique Eset. Ce client BitTorrent gratuit, qui permet de télécharger des fichiers (vidéo, sons…) est l'un des plus utilisés.
Cette fois l'éditeur propose une procédure à suivre si vous avez été piégé en téléchargeant la version 2.92 du logiciel entre le 28 et le 29 août. Si vous avez un doute, n'hésitez pas à suivre cette procédure.
Comme l'explique l'équipe de Transmission sur son site, des pirates se sont introduits dans ses serveurs et ont remplacé le logiciel par une version modifiée contenant un *malware* baptisé « OSX/Keydnap ». Ce logiciel malveillant permet, selon Eset, de dérober des mots de passe et d'installer une porte dérobée sur les ordinateurs touchés, permettant d'y avoir accès en permanence.

Un précédent avec un logiciel de racket

Tous les utilisateurs de Transmission ne sont pas concernés : seules les personnes ayant téléchargé la version 2.92 du logiciel entre le 28 et le 29 août risquent d'avoir par la même occasion installé le malware sur leur ordinateur. Ni Eset, ni Transmission n'ont précisé combien de personnes cela représentait. L'équipe du logiciel souligne toutefois que les mises à jour automatiques ne comprenaient pas ce malware.
Transmission dit avoir « *immédiatement* » supprimé la version piratée de son serveur après avoir découvert son existence, « *soit moins de vingt-quatre heures après que le fichier a été mis en ligne* ». Son site a publiéune marche à suivre pour les personnes ayant téléchargé le logiciel corrompu.
En mars, Transmission avait été victime du même type de piratage : le logiciel avait été remplacé sur le site par un *ransomware*, un logiciel de racket qui verrouille l'accès aux fichiers de sa victime et exige de l'argent en échange du déblocage de l'ordinateur.
Source : Le Monde

Réagissez à cet article

Original de l’article mis en page : Le logiciel de téléchargement Transmission à nouveau piraté

Alerte : Un canular sur Facebook qui diffuse de fausses informations terroristes

Alerte : Un canular sur Facebook qui diffuse de fausses informations terroristes

---

Les chercheurs ESET ont découvert une arnaque qui cible les utilisateurs de Facebook. D'abord répandu en République Tchèque et en Slovaquie, elle pourrait se propager dans d'autres pays

Les utilisateurs de Facebook en République Tchèque et en Slovaquie font face à une vague de fausses informations sur une attaque meurtrière à Prague. Quand l'utilisateur clique sur le canular, il est redirigé vers une page Internet de phishing qui essaye de le tromper en l'incitant à partager ses identifiants Facebook.

« D'après ce que nous savons à propos de cette campagne, l'attaque pourrait se propager dans plusieurs autres pays » met en garde Lukáš Štefanko, Malware Researcher chez ESET.

Cette prétendue attaque terroriste est facile à discréditer car la photo publiée ne ressemble pas à Prague, ni à aucune autre ville d'Europe. Malgré cela, l'arnaque se diffuse rapidement. « Les utilisateurs de Facebook partagent fréquemment des histoires sans les avoir lues. Les campagnes d'arnaques, si elles font appel à l'émotion, réussissent étonnamment bien à cause de notre empathie naturelle » commente Lukáš Štefanko.

Peu après le lancement de la campagne, Facebook a commencé à stopper les pages de phishing utilisées dans cette campagne. Les solutions de sécurité ESET sont conçues pour bloquer les pages Internet de phishing liées à ce type d'escroquerie ainsi que d'autres domaines enregistrés par cette même personne.

« Au cours des dernières semaines, il y a eu 84 domaines enregistrés par la même personne. La plupart d'entre eux possède une fonction de phishing, tandis que d'autres pourraient être utilisées à l'avenir lors d'une attaque à plus grande échelle » ajoute Lukáš Štefanko.

Voici les recommandations des experts ESET pour ceux qui pensent avoir été escroqué en partageant leurs identifiants Facebook :

– Changez votre mot de passe Facebook et utilisez les deux facteurs d'authentification fournis par Facebook

– Si vous avez utilisé le même mot de passe pour plusieurs services, changez-le partout – et mettez un terme à cette pratique très dangereuse.

Denis JACOPINI vous recommande les outils de protection suivants :

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

Original de l’article mis en page : Boîte de réception – denis.jacopini@gmail.com – Gmail

L’un des outils préférés des cybercriminels mis à mal par un coup de filet ?

L’un des outils préférés des cybercriminels mis à mal par un coup de filet ?

Karspersky publie aujourd'hui sur son blog un compte rendu d'une enquête des autorités russes à laquelle ils ont collaboré. Celle-ci a permis l'arrestation en juin d'un groupe de 50 cybercriminels, baptisés Lurk, qui opéraient notamment l'Angler exploit kit.

L'Angler Exploit Kit connaissait ces dernières années une popularité redoublée. Ce couteau suisse du cybercriminel était une plateforme utilisée pour infecter les machines de victimes : en l'installant sur un serveur et en amenant la cible à se connecter à ce serveur via un navigateur par exemple, le cybercriminel pouvait avoir recours à tout un éventail d'exploits fournis par les créateurs du kit pour tenter d'infecter la machine de la victime.

Simple à utiliser, évolutif et souvent à jour avec les derniers exploits et dernières vulnérabilités découvertes, l'Angler Exploit Kit dominait naturellement le marché. Mais en juin 2016, l'utilisation de cet outil par les cybercriminels a soudainement chuté sans véritable explication.

De nombreux observateurs avaient néanmoins fait le lien entre l'arrestation d'un groupe de 50 cybercriminels par les autorités russes et la soudaine disparition de l'Angler Kit. Dans une longue note de blog, Ruslan Stoyanov, dirigeant de l'unité investigation chez Kaspersky confirme cette théorie et détaille les 5 années passées sur la piste de ce groupe de cybercriminels de haute volée qui avaient été baptisés « Lurk ».

Le nom du groupe Lurk vient du premier malware repéré par Kaspersky en 2011. Celui-ci se présentait sous la forme d'un malware bancaire sophistiqué, qui visait principalement les logiciels bancaires afin de procéder à des virements frauduleux en direction des cybercriminels. Swift a connu plusieurs versions et évolutions, allant parfois jusqu'à fonctionner entièrement in memory pour éviter la détection.

Le malware Lurk se présentait comme un logiciel modulaire, pouvant embarquer plusieurs modules capables de réaliser des actions différentes, mais toujours orientées vers le vol de données bancaires et l'émission de virements frauduleux depuis les machines infectées.

Une petite PME sans histoire

« Avec le temps, nous avons réalisé que nous étions face à un groupe d'au moins 15 personnes. (…) Cette équipe était en mesure de mettre en place le cycle complet de développement d'un malware : à la fois sa conception, mais aussi la diffusion et la monétisation, à l'instar d'une petite entreprise de développement logiciel » explique Ruslan Stoyanov. Et le groupe Lurk avait également un autre atout de taille dans sa poche : exploitant leur renommée parmi les cybercriminels russophones, ils avaient commencé à louer les services de leur plateforme d'exploit, baptisée Angler Kit.

Cet exploit kit était à l'origine utilisé pour diffuser le malware bancaire Lurk, mais face aux mesures de sécurisation mises en place par de nombreuses banques, les revenus déclinants du groupe les ont forcés à diversifier leur activité. Les premières détections d'Angler Kit remontent à 2013, mais ce kit vendu en Saas par les cybercriminels du groupe Lurk a rapidement gagné en popularité.

Les créateurs du Blackhole kit ont été arrêtés en 2013, ce qui a laissé au nouveau programme du groupe Lurk un boulevard pour devenir le nouvel exploit kit préféré des cybercriminels. Dès le mois de mai 2015, celui-ci dominait largement le marché. Angler Kit pouvait être loué par d'autre groupe de cybercriminels qui s'en servaient pour diffuser différents types de malwares allant du ransomware au traditionnel trojan bancaire.

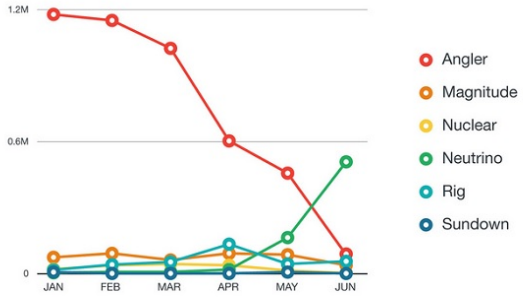


Figure 3: Number of times exploit-kit-hosting URLs were accessed in the first half of 2016

Mais le 7 juin, les autorités russes sont parvenues à arrêter les cybercriminels cachés derrière ce système. Kaspersky explique avoir collaboré avec les autorités afin de mener cette investigation, notamment via de l'échange d'informations compilées par la société sur le groupe. Un processus qui semble avoir été long et difficile, mais qui aura finalement porté ses fruits : l'Angler Kit est hors service et peut maintenant laisser la place… au nouvel exploit kit à la mode.

Selon les données récentes compilées par la société Trend Micro, l'exploit kit Neutrino aurait maintenant le vent en poupe et profiterait le plus de la retraite anticipée de son concurrent. Un de coffré, dix de retrouvés ?

Article original de Louis Adam

Réagissez à cet article

Original de l’article mis en page : L’un des outils préférés des cybercriminels mis à mal par un coup de filet ? – ZDNet