D’où vient le danger des Objets connectés ?

	D’où vient le danger des Objets connectés ?

Le développement des objets connectés s'accélère de plus en plus tandis que la mise en place de moyens de sécurité reste quant à elle beaucoup plus discrète… Tout le monde connaît le récit mythique du cheval de Troie, alors ne sommes-nous pas en train de danser sur ce qui va causer la perte de notre identité à chacun ? Qu'en est-il des normes de sécurité dans le domaine des objets connectés ? Comment pouvons-nous protéger nos données personnelles ?

Deux étudiants en médecine, ont pointé du doigt les failles que pourraient comporter certains objets connectés, dans des actions spectaculaires : prendre le contrôle d'un Pacemaker à distance ou encore désactiver les freins d'une voiture connectée. Ces actions coups de poing mettent à nu les faiblesses que comportent certains objets connectés face à des hackers malveillants. En effet, c'est précisément là que ce situe le paradoxe des nouvelles technologies qu'utilisent les objets connectés… Car s'ils sont conçus pour nous faciliter le quotidien, ils peuvent au contraire nous faire beaucoup de mal et en particulier à nos données personnelles ! Pour pouvoir se protéger, il faut avant tout comprendre cette technologie et adopter quelques habitudes très utiles.

Tout objet connecté peut être hacké

Pour comprendre comment une balance connectée peut devenir notre ennemi numéro 1, il faut d'abord comprendre comment cheminent des data (c'est-à-dire les données personnelles qui sont recueillies pendant l'utilisation de l'objet connecté) vous concernant, quels en sont les tenants et les aboutissants et où sont stocké ces données.
Il existe trois principaux canaux par lesquels voyagent nos data : les réseaux Wifi, le Bluetooth et les réseaux cellulaires pour objets connectés (Sigfox et Lora sont deux des principaux acteurs de ces réseaux).
Ces données sont ensuite acheminées jusqu'aux serveurs du fabricant ou du développeur de l'application pour ensuite revenir vers vous avant de repartir sur le Cloud… Au milieu de tous ces voyages, il devient très facile de voler ou de prendre le contrôle de vos objets, surtout si vous passez par un réseau public.

Le hackage est une menace très sérieuse à prendre en compte

En 2015, on a constaté une augmentation de 50 % de la cyber-criminalité en France ! Les concepteurs et développeurs d'objets connectés nous parlent sans cesse de nouveautés incroyables et parfaites pourtant comment celles-ci sont-elles sécurisés ? Est-ce que les différents fournisseurs appliquent ou suivent des normes ou une réglementation officielle pour sécuriser le matériel de fabrication ? Il semble qu'il n'y ai pas encore de législation officielle qui soit mise en place, même si la CNIL (Commission Nationale de l'Informatique et des libertés) s'est dernièrement attelé au sujet lors du Forum International de la cyber-sécurité.

Sécurité des objets connectés

C'est lors des voyages des data que celles-ci sont les plus vulnérables.
Mais le problème reste entier tant que les données qui voyagent ne seront pas cryptées… Ces données personnelles récoltés par les objets connectées peuvent avoir un intérêt économique pour certaines sociétés.
Ainsi, votre balance connectée peut en dire long sur vos habitudes alimentaires, votre traqueur de sommeil connecté peut donner, lui aussi, de précieuses informations sur vos habitudes de vie quotidienne. Ces données qui peuvent se monnayer très cher favorisent le profilage ciblé pour les publicités notamment et vous enlever petit à petit la liberté d'acheter ce qui vous plaît et non pas ce que l'on vous a suggéré. Le reste des data qui vous concerne, comme vos données bancaires ne sont, également, pas à l'abri d'un hackeur qui chercherait à vous voler de l'argent sans toucher à votre porte-monnaie !

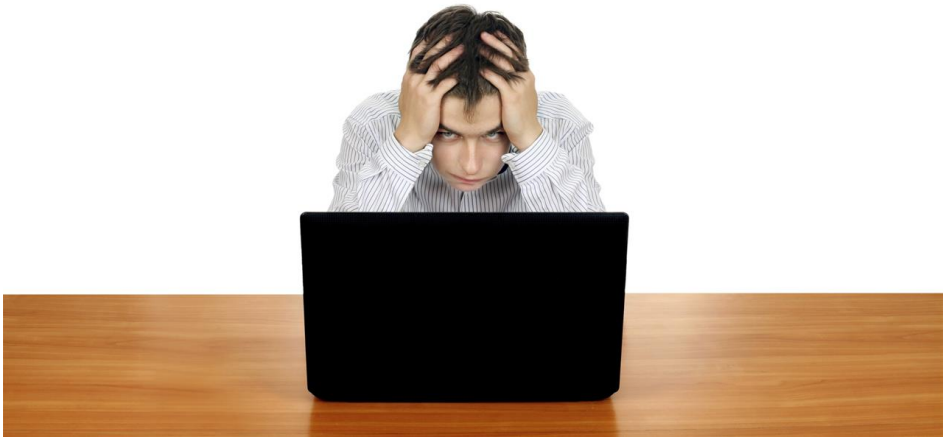
Optimisez la sécurité de vos objets connectés

Face aux deux risques majeurs de la reprise malveillante de vos données personnelles : l'utilisation commerciale et le piratage des donnés personnelles, vous pouvez adopter quelques gestes simples pour augmenter la sécurité de vos data. Si les objets connectés s'avèrent être dans de nombreux cas, un formidable assistant dans la vie quotidienne pour surveiller votre alimentation, votre sommeil, … Au contraire, s'ils sont mal connus ou utilisés d'une mauvaise manière, ils peuvent devenir très dangereux pour le particulier. Vous ne devez pas oublier qu'il est essentiel de comprendre comment fonctionnent ces technologies pour en profiter au maximum sans crainte.
Dans un premier temps, vous devez lister tous les objets connectés en activité dans votre maison et déterminer pour chacun d'entre-eux à quoi ils sont connectés et par quel biais (Wifi ou Bluetooth ou réseau cellulaire). Par cet inventaire un peu minutieux mais très utile, vous pourrez contrôler le cheminement de vos données personnelles et savoir quel objet connecté communique par des biais peu sécurisés. Pour que votre sécurité soit optimale, vous devez également effectuer régulièrement des mises à jour en ce qui concerne la sécurité et surtout changer régulièrement les mots de passe et vos identifiants. Il ne faut pas oublier que même si vos objets connectés restent dans votre maison, les data qu'ils produisent voyagent eux sur le net et donc dans le monde !

Réagissez à cet article

Source : *IOT et sécurité : ne laissez plus le cheval de Troie entrer chez vous*

Après FREAK, une nouvelle faille dans le chiffrement des connexions



Après FREAK, une nouvelle faille dans le chiffrement des connexions

Une nouvelle faille de sécurité vient de remonter à la surface : #Logjam. Né des cendres de FREAK, elle reprend le même principe de fonctionnement et permet d'établir une connexion chiffrée avec une clé trop petite pour être réellement efficace.

Au début du mois de mars, la #faille FREAK secouait Internet, pour plusieurs raisons. Tout d'abord, car elle permettait (et permet toujours) d'intercepter des échanges de données chiffrés entre un serveur et un navigateur. Ensuite car il s'agissait d'un reliquat des années 90 lorsque les États-Unis limitaient l'exportation des systèmes de chiffrements à 512 bits maximum (voir cette actualité pour plus de détail). Bien évidemment, bon nombre de serveurs et de navigateurs avaient été rapidement mis à jour suite à cette découverte.

Il convient néanmoins de relativiser puisqu'il faut procéder à une attaque de type « homme du milieu » pour l'exploiter, et donc être sur le même réseau (un « hot-spot » Wi-Fi par exemple), ce qui n'est pas toujours des plus pratiques. On est loin de la portée de Heartbleed par exemple, qui permettait à n'importe qui de lire des données directement dans la mémoire d'un serveur (identifiant, mot de passe, carte bancaire, etc.).

De FREAK à Logjam, toujours la même histoire de chiffrement « faible »

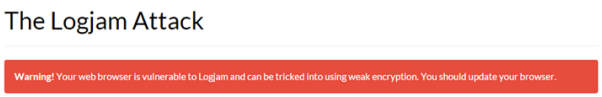
Mais une faille peut en cacher une autre et voilà désormais qu'il est question de Logjam. Elle est détaillée dans ce document, signé par des chercheurs de l'INRIA de Paris et de Nancy, de l'université de Pennsylvanie, de Johns Hopkins, du Michigan et de chez Microsoft Research. Selon les chercheurs, « *cette attaque rappelle FREAK, mais elle est due à une faille dans le protocole TLS plutôt qu'à une vulnérabilité dans son implémentation, et elle cible un échange de clés Diffie-Hellman plutôt que d'un échange de clés RSA* ».

Avec la faille FREAK et l'utilisation de la fonction « export RSA », un serveur répond avec une clé RSA de 512 bits, tandis qu'avec Logjam et « DHE_EXPORT », serveur et navigateur procèdent à un échange de clés via le protocole Diffie-Hellman, mais dans des groupes de 512 bits seulement… ce qui n'est pas suffisant pour résister à une attaque. On notera que ce problème avait déjà été évoqué par certains il y a plusieurs mois. La situation n'est donc pas nouvelle, mais elle prend une autre tournure.

Serveurs et navigateurs doivent se mettre à jour

Là encore, le problème concerne les navigateurs et les serveurs : il suffit que l'un des deux n'accepte pas un groupe de 512 bits pour que l'attaque échoue. De plus, et comme avec FREAK, il faut être sur le même réseau pour que cela fonctionne via une attaque de l'homme du milieu, ce qui limite évidemment la portée, mais n'enlève rien à sa dangerosité.

Du côté des navigateurs, Internet Explorer ne semble pas vulnérable si l'on en croit l'outil de test proposé par le site WeakDH.org, mais Chrome et Firefox le sont. Adam Langley, un cryptanalyste qui travaille chez Google, s'est exprimé sur le sujet sur l'un des forums du géant du web : « *En se basant sur leur travail, nous avons désactivé TLS False-Start avec Diffie-Hellman dans Chrome 42, qui est la version stable depuis plusieurs semaines maintenant* [NDLR : on est passé à Chrome 43 depuis ce matin, mais cela ne change rien sur le principe]*. Cette attaque sur les serveurs vulnérables sera un peu plus difficile* ».



Passer à 1 024 bits minimum, voire mieux à Diffie-Hellman sur des courbes elliptiques

Pour autant, cela n'est pas encore suffisant et Adam Langley ajoute que « *le tronc commun du code de Chrome changera afin d'imposer une nouvelle taille de 1024 bits pour Diffie-Hellman. Même si cela entraînera des problèmes pour certains sites, le travail d'aujourd'hui montre que nous ne devrions pas considérer de tels sites comme sécurisés de toute manière* ». Il précise que « *ce changement est en bonne voie d'être inclus dans Chrome 45* », mais que le calendrier pourrait être plus rapide.

Mais tout cela ne sera probablement qu'une solution temporaire. En effet, les chercheurs à l'origine de la publication de Logjam indiquent qu'un groupe de 1 024 bits peut être « cassé » par un pays ayant suffisamment de moyens (on pense notamment à la NSA qui décrypte à tout-va), et cela ne fera qu'empirer avec le temps. Le cryptographe de Google rejoint cette conclusion : « *Un minimum de 1024 bits ne suffit pas sur le long terme. Malheureusement, parce que certains clients ne prennent pas en charge les groupes de DH supérieurs à 1024 bits, et parce que TLS ne négocie pas spécifiquement certains groupes, il serait très problématique de pousser cette limite au-dessus de 1024. Alors que nous approchons de l'élimination du chiffrement RSA sur 1024 bits, nous nous interrogeons de manière plus générale sur la prise en charge des groupes non elliptiques DHE dans TLS* ». Cela laisse entendre que cette méthode pourrait disparaitre à terme, en tout cas chez Google.

Il existe en effet une version plus sécurisée de ce protocole : ECDHE pour Elliptic curve Diffie–Hellman (ou bien encore Diffie-Hellman sur des courbes elliptiques). Pour Google, « *les serveurs qui utilisent actuellement DHE devraient se mettre à jour et passer à ECDHE. Si cela est impossible, utilisez au moins DHE avec des groupes de 1024 bits et ne soyez pas trop surpris si Chrome commence à utiliser du chiffrement RSA avec votre site dans le futur* ».

Un guide des bonnes pratiques et un site pour tester navigateurs et serveurs

Cette recommandation est d'ailleurs également faite par l'équipe de chercheurs qui a mis en ligne un petit guide du déploiement de Diffie-Hellman, ainsi qu'un outil de test. Il recommande de désactiver les fonctions Export Cipher Suites, déployer un système de Diffie-Hellman sur des courbes elliptiques et utiliser un groupe fort et unique pour chaque serveur.

Comme toujours, on devrait voir arriver une série de correctifs dans les prochaines semaines, à la fois côté navigateur et serveur. Cela ne devrait pas tarder puisque les principaux concernés ont été mis au courant avant que la faille ne soit rendue publique.

Réagissez à cet article

Source : *Logjam : après FREAK, une nouvelle faille dans le chiffrement des connexions – Next INpact*

La boîte à outils des gendarmes du Net pour lutter contre la Cybercriminalité

La boîte à outils des gendarmes du Net pour lutter contre la Cybercriminalité

Installé au sein du pôle judiciaire de la gendarmerie nationale à Cergy-Pontoise, le centre de lutte contre les criminalités numériques (C3N) utilise une palette d'outils pour patrouiller sur le web et détecter toutes sortes d'infractions en ligne.
Depuis un an, l'unité lutte de manière active contre la propagande djihadiste et l'apologie du terrorisme. Elle s'est dotée pour cela de nouveaux outils et a renforcé ses équipes.
« Nous sommes un peu la Bac du net. Notre travail consiste à patrouiller sur Internet pour détecter des infractions », explique le colonel de gendarmerie **Nicolas Duvinage**, chef du centre de lutte contre les criminalités numériques. Cette entité, baptisée le **C3N**, rassemble 35 militaires. Elle est installée au Pôle judiciaire de la gendarmerie nationale (**PJGN**), dont les nouveaux locaux se situent à Cergy-Pontoise (Val d'Oise).
Le C3N mène trois principales missions : il anime et coordonne le réseau **CyberGend,** déployé sur tout le territoire, effectue du renseignement criminel (pour réaliser une cartographie et une typologie des auteurs et des victimes et détecter les modes opératoires émergents) et réalise des enquêtes judiciaires pour détecter les fameuses infractions commises en ligne. Dans le cadre de cette mission, les gendarmes interviennent dans plusieurs cas : pour les atteintes aux stades (attaques informatiques), les atteintes aux biens (contrefaçon), et les atteintes aux personnes (porno-pédographie). *« Depuis janvier 2015, nous participons également de manière active à la lutte contre la propagande djihadiste et l'apologie du terrorisme. Nous nous inscrivons dans une activité plus pérenne dans ce domaine»,* confie le colonel Nicolas Duvinage, avant de poursuivre : *« Le but n'est pas simplement de fermer un site ou de retirer des tweets, mais d'identifier les auteurs des tweets et de les interpeller pour les juger ».*

OsintLab pour patrouiller sur Twitter
35 personnes pour patrouiller sur la toile cela fait peu… Les équipes se sont donc équipées d'une palette d'outils de surveillance automatique ou semi-automatique. Un investissement logiciel qui représente plusieurs centaines de milliers d'euros par an. Parmi ces outils, le logiciel **OsintLab** développé par **Thales**et acheté en 2015. Celui-ci permet de sillonner **Twitter** en s'appuyant sur des mots clefs. *« Cet outil nous a permis de mener plusieurs dizaines d'enquêtes judiciaires au travers desquelles nous avons pu identifier des personnes radicalisées »,* assure le colonel. Après avoir « logé » ces personnes, les équipes du C3N transfèrent le dossier à l'échelon spécialisé ou l'échelon territorial compétent, qui se chargera de réaliser l'interpellation.

Advestisearch pour identifier les primo-diffuseurs
Le C3N utilise également le logiciel **Advestisearch** d'**Hologram Industries**, qui permet de rechercher et d'identifier des contenus illégaux et illicites sous forme de texte, d'image ou de vidéo. *« Grâce à une image fournie en entrée, nous pouvons trouver en sortie des images similaires. Par exemple, lorsqu'une équipe de gendarmes récupère une vidéo de 10 secondes, l'outil nous permet de retrouver la vidéo complète. Cela nous permet aussi de détecter les primo-diffuseurs »,* détaille le colonel.

Et bientôt un *Scraper Deep Web* maison
Le C3N n'utilise pas uniquement des logiciels « sur étagère », mais développe également ses propres outils. L'unité s'attèle, par exemple, à mettre au point son propre *Scraper Deep Web*, un outil qui permet de collecter automatiquement des petits morceaux d'information sur des réseaux comme **TOR.** Une démarche qui rappelle le projet **Memex** mené par la **Darpa.** L'agence pour les projets de recherche avancés de défense américaine a, en effet, récemment créé un « *Google du Deep Web* » afin d'aider la police dans ses enquêtes en tout genre.

Le C3N s'emploie également à scruter les jeux en ligne. *« Les auteurs détournent de plus en plus les jeux en ligne comme **Clash of Clan**, **Call of Duty** ou encore **Oh My Dollz** »*, assure le spécialiste. *« Sur Clash of Clan, par exemple, nous avons identifié en 2015 plusieurs dizaines de cas d'apologie du terrorisme et de menaces d'attentats ».*
Outre les logiciels, le C3N mise également sur les compétences humaines. L'unité a récemment recruté plusieurs officiers commissaires, dont un docteur en informatique, un ingénieur en électronique et un universitaire spécialiste des systèmes d'information.

Réagissez à cet article

Source : *Cybercriminalité : la boîte à outils des gendarmes du Net*

Mots de passe : nos conseils pour une sécurité maximum

Mots de passe : nos conseils pour une sécurité maximum

password, admin, 123456, abcdef, qwerty, j'en passe et des meilleures… Voilà des mots de passe encore bien utilisés si l'on en croit le palmarès 2013 des 25 mots de passe les plus fréquents (publié par la société SplashData, éditrice de logiciels). Mais de véritables passoires en termes de sécurité ! A l'heure du cloud et des services Web qui numérisent toujours un peu plus nos vies, la vigilance ne saurait souffrir de négligences. De l'importance de sécuriser ses mots de passe, nous vous expliquons le pourquoi et le comment.

Paranoïa, quand tu nous gagnes…

On a beau être d'un naturel plutôt stoïque, la lecture du rapport P@$$1234: the end of strong password-only security publié en janvier 2013 par le cabinet d'expertise Deloitte donne tout de même quelques sueurs froides… Il s'appuie sur un travail intéressant de Mark Burnett (du site Xato.net), lequel a décortiqué une liste de 6 millions de duos login plus mot de passe uniques pour en extraire des statistiques.

- 98,8 % de cette base d'utilisateurs emploient les 10 000 mots de passe les plus fréquents ;
- 91 % se concentrent sur 1 000 mots de passe ;
- 40 % font avec 100 mots de passe ;
- 14 % (soit 840 000 personnes tout de même) piochent dans le top 10 !

Et le problème de ces mots de passe ultra bateau, dont « password » et « 123456 », c'est qu'ils représentent le degré zéro de sécurité, puisqu'ils seront les premiers à être testés par tout hacker qui se respecte. Le souci de sécurité n'est visiblement pas encore rentré dans toutes les têtes…

Pour mieux se protéger de l'ennemi, il faut tenter de le comprendre. Comment les hackeurs fonctionnent dans les grandes lignes ? Quatre scenarii sont à envisager : le piratage en direct, le vol de bases de données, le phishing (ou plus globalement le *social engineering* précise Paul Rascagnères, analyste malware chez l'éditeur d'antivirus G DATA) et les virus.

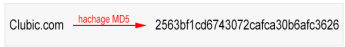
Le premier, qui consiste à tester tous les mots de passe possibles et imaginables dans une interface de connexion sur la base d'un identifiant connu, n'est plus possible aujourd'hui ou très rarement. Cela, parce que la grande majorité des sites sérieux bloquent les comptes au bout de quelques tentatives ratées, trop peu nombreuses même pour un mot de passe évident (quoique avec password et 123456…).

Non, le gros des dangers tient dans le vol, les virus et le *social engineering*. Pour ce dernier, une sorte de vol avec consentement non éclairé, la complexité d'un mot de passe n'a pas d'intérêt : le hackeur se fait passer pour quelqu'un d'autre (email, coup de fil ou faux site officiel), et s'il parvient à duper l'utilisateur, il en profite pour récupérer ses identifiants, en clair. La pratique est courante, les données sont ensuite utilisées ou revendues sur des marchés parallèles. Le seul remède dans ce cas, c'est la vigilance. Idem pour l'aspect virus, un malware avec keylogger peut intercepter vos saisies au clavier ou chiper les identifiants stockés dans le navigateur par exemple : votre ordinateur doit être protégé par un antivirus, à jour, et en programmant des analyses régulières.

? Un hash qui part d'autant plus vite en fumée que le mot de passe est simple ?

C'est en matière de vol qu'il est intéressant de comprendre les mécanismes. Tous les couples identifiants / mots de passe des services Web sont stockés sur les serveurs des entreprises respectives, et forment ainsi autant de bases de données. Ces vols sont assez ponctuels mais malheureusement massifs (par milliers voire millions d'entrées). Très rarement (et normalement pas en France puisque c'est illégal), ces bases de données sont stockées en clair. Si dérobade il y a, la complexité du mot de passe sera vaine.

Mais dans la majorité des cas, les identifiants et mots de passe sont hachés, c'est-à-dire brouillés par un algorithme. Quand quelqu'un veut se connecter à son service, le mot de passe qu'il entre est également haché en temps réel, puis comparé à celui stocké sur les serveurs. Les hackeurs qui se procurent pareilles bases de données vont devoir utiliser des logiciels spécifiques pour déterminer quelle fonction de hachage (hash en anglais) a été utilisée, après quoi ils peuvent automatiser les tests. Tests qui vont consister à choisir un mot, le hacher, le comparer à l'empreinte hachée de la base de données volée : s'il y a correspondance, le mot de passe est trouvé, sinon il faut tester un autre mot, etc. Un hash qui part d'autant plus vite en fumée que le mot de passe est simple.



En hachant un mot via un algorithme, on obtient une empreinte de ce type. Il existe plusieurs algorithmes, proposant des niveaux de sécurité plus ou moins élevés : MD5, SHA-1, SHA-2, etc…

Le hasard fait parfois bien les choses, mais les statistiques les font encore mieux. Pour éviter de tâtonner au doigt mouillé, les hackeurs recourent à des dictionnaires, ou mieux encore, à des listings de mots de passe qui ont été établis au fil des différents vols de données, comme la base du réseau communautaire RockYou.com et ses 32 millions d'entrées évaporées dans la nature en 2009. De vrais mots de passe, couramment employés, et qui ne changent pas beaucoup, comme en témoigne la constance des palmarès des mots de passe les plus fréquents, d'une année sur l'autre. Les cas de vols de données ne manquent pas : Ebay,Orange, Domino's Pizza ou encore Adobe pour les exemples les plus récents.

Vends forfait 4G pas cher, avec livraison à domicile. Seul moyen de paiement accepté : l'abonnement annuel.

Les listings contiennent des mots simples, les logiciels pirates proposent donc des règles complexes. Mais faciles à mettre en oeuvre d'après le journaliste Nat Anderson. Son expérience est instructive. En tentant de se mettre dans la peau d'un hacker, il a potassé le fonctionnement des logiciels pirates, et notamment de Hashcat, qui sont, sans surprise, très bien conçus.

En quelques clics, on peut étoffer la recherche, de sorte à ce que sur un mot de passe comme « clubic » (à tout hasard), le logiciel teste également des ajouts de chiffres ou de lettres (« clubic10 » ou « clubicz »), mais aussi l'ordre inversé (« cibulc »), les ajouts de préfixes et suffixes courants (man, 123, mad, me…), la version *leet*, c'est-à-dire avec des caractères alphanumériques ASCII (« (|_ |_| |3 | (») voire des inversions de lettres. De quoi multiplier les chances du malfaiteur d'arriver à ses fins.


Le logiciel Hashcat

? Un mot de passe à 8 caractères hacké en 5 h 30 ?

Plus efficace encore mais exigeante en ressources, la bonne vieille attaque de force brute. Sur une quantité donnée de caractères, mettons six, la technique un brin bourrine consiste à hacher et tester « aaaaaa », puis « aaaaab », etc. Sachant qu'un clavier français peut produire 142 caractères (avec tous les accents, la casse, les symboles, les chiffres, et encore 103 si on exclut les accents) et que la statistique est exponentielle, ça nous fait 8 198 418 170 944 de combinaisons possibles (8 200 milliards pour ceux qu'autant de chiffres perturberait). Dans l'exemple donné par l'étude du cabinet Deloitte, un mot de passe à 8 caractères (6,1 millions de milliards de possibilités sur un clavier américain à 94 caractères) pourrait être hacké en 5 h 30 par une configuration dédiée haut de gamme (estimée à 30 000 $ en 2012), mais en près d'un an avec un PC correct de 2011.

Représentation visuelle de ces chiffres astronomiques

Le petit point noir, c'est le nombre de combinaisons à 8 caractères, le gros point bleu c'est avec 10 caractères. Les joies de l'exponentiel !

Voilà donc la clef : plus un mot de passe est complexe (avec des caractères spéciaux, un séquençage aléatoire, etc.) et long, plus le hacker aura du fil à retordre. Rien qu'en passant à 10 caractères, courbe exponentielle oblige, on fait grimper les combinaisons sur un clavier français à 3 333 369 396 234 118 349 824 (3 333 milliards de milliards !!!). La même machine de compétition mettrait alors 343 ans pour tester toutes les combinaisons… A cette parade, les hacker répondent par le crowd-hacking : ils confient des fragments de calculs à faire à des milliers de PC normaux infectés (les fameux PC zombies). C'est supposé aller beaucoup plus vite ainsi, mais bon, les hackers préfèrent tout de même les mots de passe courts et basiques.

? nous peinerions à retenir plus de sept chiffres dans notre mémoire à court terme ?

Le remède est simple, sa mise en oeuvre plus délicate. D'après une étude de l'Université de Toronto que cite le rapport Deloitte, les êtres humains limités que nous sommes peinerions à retenir plus de sept chiffres dans notre mémoire à court terme, et même plus que cinq en prenant de l'âge. L'ajout de symboles, de lettres majuscules et minuscules produirait un mix encore moins aisé à retenir. Le rapport se fait plus accablant en ajoutant que la nature humaine a tendance à suivre des schémas de pensée limités par rapport aux possibilités offertes. La majuscule ? En première position dans les mots. Les chiffres ? À la fin. Des 32 symboles présents sur un clavier américain ? Une demi-douzaine seulement est utilisée. De quoi rendre l'aléa théorique plus prédictif pour les hackers. Rien de nouveau cependant. A moins que… le rapport ne pointe du doigt un nouveau frein, imputable aux usages mobiles. L'absence ou la moindre accessibilité des caractères spéciaux sur les claviers des smartphones amène le nomade à simplifier son mot de passe. Tout comme le temps de saisie supérieur qui inciterait un quart des personnes sondées à utiliser un mot de passe plus court pour gagner du temps. De 4 à 5 secondes pour taper un mot de passe de 10 caractères sur un clavier standard d'ordinateur, il faudrait entre 7 et 30 secondes pour faire la même chose depuis un smartphone tactile.

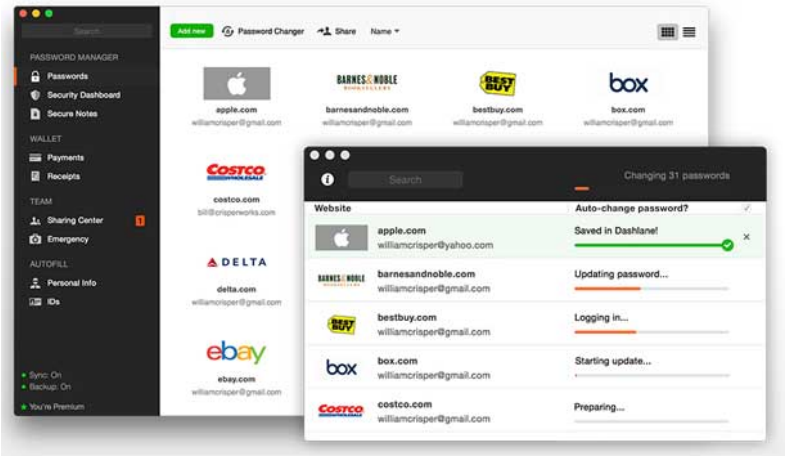
Réagissez à cet article

Source : *Mots de passe : nos conseils pour une sécurité maximum*

Dashlane : 500 mots de passe modifiés en un clin d’oeil

Dashlane : 500 mots de passe modifiés en un clin d’oeil

La nouvelle version de l'outil français des gestion des mots de passe propose d'automatiser la gestion des mots de passe. De quoi soulager des utilisateurs toujours plus sollicités sur le terrain de la sécurité.



La multiplication des services en ligne fait exploser le nombre de mots de passe utilisés par les professionnels. Au point de poser des problèmes de mémoires insolubles. Google réfléchit à les remplacer grâce au smartphone.

Dashlane propose le changement automatique de mot de passe pour 500 sites Web. (Source : Dashlane)

La pépite Dashlane propose elle une alternative au stockage manuel de plusieurs mots de passe en automatisant le stockage et la modification des mots de passe. Et la dernière version de l'outil permet de le faire pour 500 sites (au lieu de 75 jusqu'alors) et services web en un seul clic, avec la fonctionnalité Password Changer.

Banque et mot de passe

8 formats de documents sont désormais pris en charge : les applications, les bases de données, les documents financiers, les documents juridiques, les abonnements, les licences logicielles et les mots de passe Wi-Fi. Autres nouveautés de cette quatrièmes version de Dashlane, 7 langues différentes sont supportées et l'interface graphique a été revue de mnière à être identique quelque soit la plateforme (Mac, PC, iOS et Android). Autre amélioration, un moteur de recherche plus performant et un affichage des résultats sous divers formats.

Côté moyen de paiement, 618 nouvelles banques internationales peuvent être utilisées dans les moyens de paiement. A noter que la version de base de Dashlane est proposées gratuitement, et que la version Premium 39,99 euros/an) permet de synchroniser les données sur mobile (nombre illimité d'appareils) et de les sauvegarder en mode sécurisé.

Réagissez à cet article

Source : *Dashlane : 500 mots de passe modifiés en un clin d'oeil*

Palmarès des mots de passe 2015

	**Palmarès des mots de passe 2015**

Comme chaque année, Splashdata dévoile les mots de passe les plus utilisés par les internautes, une liste qui est le fruit de données volées et rendues publiques. Sans surprise, « 123456 » et « password » se disputent toujours les deux premières places. Mais ce palmarès 2015 révèle aussi l'influence de Star Wars dans le choix des internautes.

Tous les ans à la mi-janvier, nous attendons avec impatience la réponse à cette question : l'humanité a-t-elle enfin compris que la plus grande des failles informatiques était un mot de passe trop simple à trouver ?
Mais cette fois encore, la déception est au rendez-vous : ces satanés « 123456 » et « password » trônent encore, là, tout en haut du classement.
Évidemment, on peut modérer ce sentiment en rappelant que la liste en question est obtenue en étudiant « seulement » deux millions de mots de passe échappés dans la nature. Comparé aux près de trois milliards d'internautes dans le monde, qui possèdent chacun plusieurs mots de passe (si, si, ça existe), cela reste faible.
Mais l'échantillon demeure représentatif, et on peut malheureusement imaginer que dans notre entourage proche, certains utilisent encore 12345678 (troisième du classement) ou même 12345 (qui rétrograde en cinquième position).

La tête de ce classement 2015 s'éloigne assez peu de celle du palmarès 2014, mais laisse tout de même de la place pour quelques nouveautés, dont le très original « welcome », directement propulsé en onzième position, immédiatement suivi par un autre promu, le très complexe « 1234567890 ».
Enfin, on note l'influence de la sortie de l'épisode 7 de *Star Wars* sur ce millésime 2015 : « princess » (en 21e position) et « solo » (23e) peuvent le laisser penser, alors que « starwars » (25e) ne laisse pas de place au doute.
Le classement en question :

- 1. 123456 (-)
- 2. password (-)
- 3. 12345678 (+1)
- 4. qwerty (+1)
- 5. 12345 (- 2)
- 6. 123456789 (-)
- 7. football (+3)
- 8. 1234 (-1)
- 9. 1234567 (+2)
- 10. baseball (-2)
- 11. welcome (nouveau)
- 12. 1234567890 (nouveau)
- 13. abc123 (+1)
- 14. 111111 (+1)
- 15. 1qaz2wsx (nouveau)
- 16. dragon (-7)
- 17. master (+2)
- 18. monkey (-6)
- 19. letmein (-6)
- 20. login (nouveau)
- 21. princess (nouveau)
- 22. qwertyuiop (nouveau)
- 23. solo (nouveau)
- 24. passw0rd (nouveau)
- 25. starwars (nouveau)

Réagissez à cet article

Source : *Palmarès des mots de passe 2015 : du classique, mais avec un peu de Star Wars*

Panorama de la Cybercriminalité en 2015 : Attaques sur tous les fronts !

Panorama de la Cybercriminalité en 2015 : Attaques sur tous les fronts !

La nouvelle édition du panorama de la cybercriminalité du CLUSIF a fait la démonstration que la crise ne touche pas les pirates informatiques bien au contraire. Ils restent toujours aussi inventifs d'autant que leur terrain de jeu s'accroit grâce à l'introduction des nouvelles technologies dans de plus en plus de domaine entre autre avec les objets connectés. En parallèle, le cyber-terrorisme s'il n'est pas encore avéré au sens d'attaque visant à des détruire des entreprises ou des infrastructures critiques se sert du net pour tisser sa toile en recrutant des futurs terroristes, en menant des actions de communication, voir en servant de support pour monter des opération sur le terrain… cette année riche en actions malveillantes laisse augurer du pire pour 2016…

Après l'introduction par Lazaro Pejsachowicz, le président du CLUSIF qui a présenté les différentes activités de l'association, le panorama a débuté. En introduction il a rappelé que le cyber-crime se porte très bien. En outre, il a annoncé qu'en juin prochain aura lieu la conférence sur les résultats de l'enquête MIPS pour Menaces Informatiques et Pratiques de Sécurité.


Fabien Cozic

Quelques astuces utilisés en 2015

Fabien Cozic, directeur d'enquêtes privées Read Team Investigation, a passé en revue quelques astuces utilisées par les pirates a commencé par la Yes Card qui a exercé ses activités en France et en Belgique. Le pirate était un ingénieur qui avait rajouté une petite puce de la carte bancaire qui permettait de valider les transactions en se substituant à la puce déjà installée.
Un groupe de pirate avait mis en place un système astucieux de déposé et de retrait des sommes. Puis une équipe en République Tchèque puis un second groupe effectuait des transactions aux Etats-Unis puis les annulait et récupérait ainsi de l'argent. Le préjudice se chiffrerait autour de 6 millions d'euros.
XCode Ghost qui a détourné le système de contrôle des applications d'Apple. Les pirates ont utilisé une faille humaine de ce système pour déposer des malwares afin de récupérer des informations
Le malwares Turla a utilisé des APT pour réaliser des écoutes en se servant des liaisons des satellites de communication.
Un malware a été conçu pour prendre le contrôle de la lunette de visé d'un fusil afin de déclencher le tir…
Pour conclure il a cité le détournement d'un jouet en utilisant le système de communication pour ouvrir les portes de garages. Ce malware a contribué à plusieurs cambriolages aux Etats-Unis.


Hervé Schauer

Le 0 Days un business juteux pour les entreprises

Loic Samain du CEIS représenté par Hervé Schauer a présenté l'évolution du business des 0 Days. La palme de l'année revient à un 0 Day sur IOS qui a été récompensé par 1 millions de $. Les systèmes de plateforme de 0 Day existent et se développent. Leurs clients sont tout d'abord les gouvernements qui veulent réaliser des écoutes, mener des attaques… Il a donné quelques exemples de prix comme par exemple 2000$ pour un 0 Day ciblant un site de ecommerce, pour Windows le prix est de 150000$… et pour IOS a atteint 1 million de $.
Le 20 mai 2015 la proposition Wassenaar sur les 0 Day a été publié et elle est déjà adopté par plusieurs pays. Une nouvelle proposition pour amender cette proposition devrait être faite en 2016. Aujourd'hui les primes aux 0 Days explosent avec des prix allant de 2000$ à plusieurs milliers de $. Ainsi, les entreprises de Bug Bounty voient leur valorisation exploser.
Ainsi, Vupen est devenu un grossiste en 0 Day et s'appelle aujourd'hui Zerodium. En janvier 2016 une faille de sécurité a été payée 100 000$ par cette entreprise pour la découverte d'une faille sur flash. Pour Hervé Schauer « 2015 est donc l'année de la professionnalisation de ce marché. »


Loïc Guezo

La cyber-diplomatie commence à émerger

Loïc Guezo, Strategist chez Trend Micro, a expliqué que l'on va vers une cyber-diplomatie avec entre autre la remise en cause de l'ICANN qui est au centre de très grandes manœuvres. On a de nombreux pays qui reconnaissent une capacité offensive sur Internet a commencé par les États-Unis, la Grande Bretagne, la Chine, la Russie et maintenant la France. En 2015, il a rappelé le cas du piratage OPM qui est une sorte de RH des agents des services spéciaux américains avec la récupération très personnel sur l'ensemble des collaborateurs. La Chine a été suspectée d'être l'auteur de ce piratage. Suite à cette accusation plusieurs arrestations ont eu lieu en Chine afin de faire diminuer les tensions entre ces deux pays. Aujourd'hui, le doute persiste sur la nature des personnes arrêtées. Le 31 décembre 2015 les autorités américaines ont ressortie une attaque sur 2009 ciblant Microsoft. Par contre Microsoft n'a pas alerté ces clients. Par ailleurs, la Russie a signé un pacte de non-agression avec la Chine mais ne signifie pas l'arrêt des opérations entre ces deux pays, il y a par contre une convergence de doctrine sur l'Internet autour de l'idée de souveraineté.
Quant à l'Iran et dans une moindre mesure à la Corée du Nord, ils ont été pointés par les Etat-Unis comme deux dangereux pays sources de piratages.
Par ailleurs, il a cité l'Accord Umbrella qui a été noté comme une grande avance en particulier Ui permet de facilité les procédures d'extradition. En France, il faut noter la publication de la Nouvelle Stratégie de la sécurité du numérique. A cette occasion, David Martinon a été nommé Ambassadeur pour la cyber-diplomatie et de l'économie digitale.
La cyber-diplomatie est devenue un élément clé de la vie politique dont l'influence géopolitique prévue dans cette nouvelle stratégie.

François Paget

Le Djiad Numérique : recrutement, endoctrinement…

François Paget a présenté pour sa part le Djiad Numérique. Lors du panorama 2004, il avait été évoqué l'utilisation d'Internet par les terroristes. Aujourd'hui, ils utilisent les réseaux sociaux et adressent plusieurs milliers de Tweet par jour. Daesh offre des conseils pour se dissimuler via par exemple les réseaux Tor, mais aussi Telegram. Ce dernier réseau social est dominant en Russie. Il permet de communiquer de façon chiffrée mais aussi de détruire les messages une fois lus. Les djihadistes se servent aussi du darknet, peut-être de Bitcoins… pour acheter des armes. Sans compter que les réseaux sociaux sont utilisés pour recruter des membres mais ce n'est pas le seul vecteur d'enrolement.
En novembre, les Anonymous se sont réveillés pour attaquer les djihadistes avec des actions parfois intéressantes, mais ils aussi ont réalisé des bévues qui ont parfois ralenties les actions des forces de police, voire aussi en attaquant des sites qui étaient en arabes mais sans aucun lien avec les terroristes.
En janvier dernier, il y a eu des défacements de sites surtout en janvier en particulier par Isis. Par contre, il y en a eu très peu après les attentats de novembre. Durant ces moments tragiques, Google a été particulièrement sollicité. Par contre, les réseaux sociaux ont servi à des élans de solidarité surtout en novembre. En revanche, Facebook a mis parfois beaucoup de temps pour fermer des sites malveillants. Quant à tweeter il a agi un peu plus rapidement, mais a laissé courir de nombreuses rumeurs. En ces périodes, il y eu de nombreuses fausses rumeurs qui ont circulé avec même des chevaux de Troie dissimulés dans certaines images.


Amélie Paget

Vers une limitation des libertés ?

Amélie Paget, consultante juridique SI HCS by Deloitte a fait le point sur les deux nouvelles lois publié en 2015 pour renforcer les pouvoir de l'Etat : la loi sur le renseignement et l'Etat d'urgence. Pour ce qui concerne l'état d'urgence il a été prorogé jusqu'au 26 février 2016. Désormais, lors des perquisitions, les agents peuvent accéder aux données stockées sur les systèmes Informatiques ou l'équipement terminal ou accessible à partir du système initial. En outre, ils auront la possibilité de copier les donner et d'effectuer des saisies en cas d'infraction. Par ailleurs un projet de loi souhaite insérer à notre Constitution, un nouvel article consacré à l'état d'urgence.
En ce qui concerne la Loi sur le renseignement, elle donne des prérogatives pour accéder aux données de connexion en les demandant aux opérateurs, aux FAI et hébergeurs.. Les agents peuvent utiliser des outils de géolocalisation et demander en temps réel aux FAI des information et documents qui transite sur le réseau. Bien sûr toutes ces actions ne peuvent s'effectuer que pour protéger les intérêts fondamentaux de la Nation, notamment pour la prévention du terrorisme. Les agents peuvent collecter des informations en échangeant sur la toile. Quant au chiffrement les opérateurs auront 72 heures pour offrir un système de déchiffrement ou directement les documents en clair.


Gérôme Billois

Objets connectés : la sécurité doit être intégré by design

Gérôme Billois, Manager Sécurité de Solucom a traité des attaques sur les objets connectés en rappelant qu'en juillet dernier deux chercheurs ont pris le contrôle à distance d'une voiture connectée. En fait, les consoles de bords sont connectées à un premier Réseau dit de confort et un second pour la conduite comme celui qui gère le régulateur de vitesse, la boite de vitesse, le volant… En fait, la console de bord est assez facile à pirater et permet de prendre le contrôle de la console de confort. Par contre, la console de sécurité est plus difficile à pirater. Par contre, avec du temps et un peu de chance selon les dires de ces deux chercheurs, la prise de contrôle sur la console de sécurité est faisable. Cette démonstration a eu des impacts médiatiques mais aussi financiers pour les constructeurs avec l'envoi de clés USB aux utilisateurs pour faire des mises à jours, heureusement à ce jour, toujours pas d'attaque sur les voitures… Toutefois il est possible d'envisager la diffusion de ramsowares qui bloqueraient les voitures…
Au delà des voitures, les jouets connectés ont fait l'objet d'attaques plus ou moins amusants avec par exemple Barbie, les téléviseurs… Par contre, d'autres attaques seraient plus graves comme celle sur des pompes à insuline, des fusils, voir des avions…
En fait, en matière de sécurité des objets connectés il y a 4 dimensions à prendre compte : ceux qui les conçoivent, ceux qui les achètent, ceux qui les conseillent et tous ceux qui vont les accueillir en particulier dans les entreprises. Il faut donc réagir en intégrant la sécurité, en protégeant notre vie privée, sans oublier les spécificités de ces objets. Demain, nous allons voir arriver les objets autonomes qui vont demain faire partie de notre quotidien avec par exemple des robots qui vont être mis dans les boutiques Nespresso, à bord des bateaux de Costa Croisières… Cela pose, de nombreuses questions juridiques.


Garance Mathias

Objets connectés : les premiers procès à l'horizon 2016

Garance Mathias en préambule de son intervention explique que nous sommes tous concernés par les objets connectés car nous en avons tous. Le droit à déjà prévu le fait que l'on est responsable de nos objets. Un grand classique du droit est qu'il s'impose à tous les acteurs : le concepteur, l'utilisateur… Par exemple, le Cloud qui relie les objets connectés n'est qu'une externalisation avec toutes les contraintes liées.
Concernant les objets connectés, il faut aussi prendre en compte les analyses d'impacts d'où la nécessité pour les fabricants d'embarquer la sécurité y design. Elle a pris l'exemple de Vtech qui avait fait l'objet d'une plainte par « UFC Que Choisir » du fait de la non-prise en compte de la protection de la vie privée.


Le Colonel Éric Freyssinet

Téléphonie mobile : le protocole SS7 mis à mal…

Le Colonel Éric Freyssinet a évoqué en premier lieu la sécurité des téléphones mobiles. Fin 2014, une conférence lors du CCC a mis en lumière une vulnérabilité dans le protocole SS7 qui permettait de rediriger des communications et d'intercepter des SMS (chiffrés). En ce qui concerne les logiciels malveillants, il y a eu peu de nouveautés. Toutefois, parmi les nouveautés on trouve Pornbroid qui bloque le téléphone sous Android qui est un logiciel assez avancés capable de se relancer une fois désinstallé. Il a aussi cité Xcode qui exploite une vulnérabilité sur IOS.
… et des attaques aux effets collatéraux redoutables
Puis, le Colonel Eric Freyssinet a présenté les conséquences d'une attaque. Il a pris l'exemple de Target dont l'attaque a coûté environ 67 millions de $ avec Visa, la même somme avec MasterCard au final cette attaque devrait coûter environ 100 Millions de $ dont 90 sont pris par son assurance.
L'attaque contre OPM qui ciblait les personnels de l'état américain par la Chine a obligé la CIA a retiré des agents basés en Chine, sans compter la notification à plusieurs millions de personnes.
Hello Kity a aussi été visé par une attaque ciblée pour récupérées données Bancaires des parents.
TV 5 Monde a été une des premières véritables attaques pour détruire une entreprise. Au final l'impact sur le SI a été faible par contre les ventes de publicité se sont effondrées et son budget sécurité a été augmenté de façon conséquente. Son PDG a témoigné dans plusieurs conférences ce qui a un effet plutôt positif.
Ashley Madison est une affaire assez complexe. On a noté quelques retombées tragique comme le suicide d'un pasteur, des démissions, des chantages… De ce fait, la CNIL a demandé aux sites de rencontre français de renforcer leur sécurité.
Pour finir, il a recommandé de prévenir les risques, être capable de décréter la survenance d'un incident et être en mesure de maitriser leur impact.
François Paget a pour sa part rappelé que les forces de police rencontrent quelques succès en arrêtant des cybercriminels partout dans le monde.

Jean-Yves Latournerie

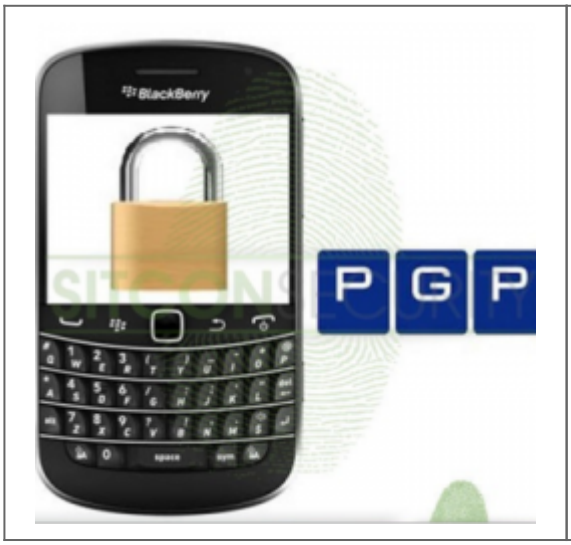
Nous passons à lutte anti-terroriste 2.0

La conclusion a été assurée par le cyber-préfet Jean-Yves Latournerie qui a félicité les intervenants et les organisateurs de ce panorama. Selon lui, il n'y a pas à ce jour d'actions en cyber-terrorisme à proprement parler. Par contre, le cyber joue un rôle très important dans la radicalisation, le recrutement et le passage à l'acte. Dans ces périodes tragiques, on apprend vite et on est en train de passer dans la lutte antiterroriste 2.0. Dans ce cadre le panorama du CLUSIF est important afin de mieux comprendre la nature de la menace de façon systémique et analytique et pouvoir ainsi anticiper les développements des actions terroristes. Il s'est félicité de voir le travail entre les forces de police et les entreprises privées se renforcer en particulier avec les principaux acteurs d l'Internet. Il note de réel progrès opérationnel entre janvier et novembre dernier. En effet, un travail méthodologique a été effectué entre ces deux périodes qui porte ces fruits aujourd'hui.
Il a conclu son intervention en rappelant que même s'il a quelques arrestations, le crime pour le moment sort le plus souvent des confrontations avec les forces de polices, toutefois, il semble que tous les acteurs d'Internet sont de plus en plus sensibiliser à ces attaques ce qui donne des espoirs pour améliorer cette situation.

Réagissez à cet article

Source : *Panorama 2015 de la Cybercriminalité du CLUSIF : Attaques sur tous les fronts ! – Global Security Mag Online*

Les Blackberry PGP déchiffrés par la Police hollandaise



Les Blackberry PGP déchiffrés par la Police hollandaise

Commercialisés par de nombreux vendeurs en ligne, les smartphones Blackberry embarquant en surcouche le standard de chiffrement de messagerie PGP seraient loin d'assurer un échange confidentiel des données. Tout du moins pour la Police hollandaise qui a confirmé être en mesure de les déchiffrer.

Les oreilles des défenseurs de la vie privée vont encore siffler. Des enquêteurs de la Police hollandaise ont en effet confirmé à Motherboard être en mesure d'accéder aux messages chiffrés envoyés depuis un terminal Blackberry sur lesquel le standard de chiffrement PGP est intégré en surcouche. « Nous sommes capables d'obtenir des données chiffrées depuis les terminaux Blackberry PGP », a fait savoir Tuscha Essed, responsable presse du Netherlands Forensic Institute (NFI), qui assiste la Police dans la recherche de preuves pour ses enquêtes en Hollande. L'information était parue initialement en décembre sur le blog misdaadnieuws.com où plusieurs documents sourcés NFI ont été publiés.

Le fait que les emails chiffrés puissent être lus et les messages effacés retrouvés, ne semble en tout cas pas perturber outre mesure les fournisseurs de Blackberry PGP. « Nous n'avons pas été affecté. Nos services sont complètement sécurisés et nous n'avons jamais été compromis », a indiqué un porte-parole de GhostPGP dans un mail à Motherboard. « Nous utilisons le dernier chiffrement PGP du moment qui est aussi impossible à déchiffrer. Nos clients sont très satisfaits du niveau de sécurité fourni », a quant à lui indiqué un représentant de TopPGP.com.

Réagissez à cet article

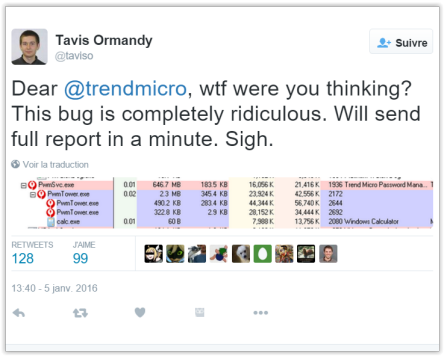
Source : *Les Blackberry PGP déchiffrés par la Police hollandaise – Le Monde Informatique*

Le coffre-fort à mots de passe de Trend Micro pas si fort

Le coffre-fort à mots de passe de Trend Micro pas si fort

L'éditeur de solutions de sécurité Trend Micro a lancé un correctif pour patcher une faille dans son logiciel Password Manager permettant à un attaquant distant de voler les mots de passe utilisateur.

Un chercheur en sécurité de Google, Tavis Ormandy, a tiré la sonnette d'alarme après avoir trouvé plusieurs failles dans le gestionnaire de mots de passe de Trend Micro, Password Manager. Ces dernières peuvent permettre à un personne malintentionnée d'exécuter du code à distance et de voler les mots de passe des utilisateurs stockés dans ce logiciel. L'éditeur japonais a confirmé ces problèmes et propose une mise à jour automatique pour les résoudre.



Ce n'est pas la première fois que Tavis Ormandy alerte l'éditeur sur l'existence de telles failles de sécurité. Se sentant frustré par un temps de réaction trop long de Trend Micro, le chercheur de Google a d'ailleurs pris la décision de poster les derniers échanges qu'il a eus avec la société. « Alors cela signifie que n'importe quel internaute peut voler tous les mots de passe en silence, autant qu'exécuter du code arbitraire sans aucune interaction utilisateur », s'est indigné Tavis Ormandy. « J'espère vraiment que vous prenez conscience de la gravité de la situation car je suis très étonné de tout cela. »

Des mots de passe utilisateurs trouvés en 30 secondes

Les utilisateurs des solutions antivirus de Trend Micro peuvent choisir d'utiliser le gestionnaire de mots de passe Password Manager afin pour exporter dedans l'ensemble de leurs mots de passe et de n'avoir plus qu'un mot de passe maître à retenir et utiliser. Les concurrents Dashlane ou LastPass proposent des services similaires. Ce gestionnaire est écrit en Javascript avec node.js et ouvre de multiples ports HTTP RPC pour des requêtes API, a précisé Tavis Ormandy. En 30 secondes, le chercheur indique avoir trouvé une requête API permettant d'accepter du code distant et également qu'une autre lui a permis d'accéder aux mots de passe stockés dans le gestionnaire. Cerise sur le gâteau, M. Ormandy a trouvé plus de 70 API de Trend Micro étaient exposées et a recommandé – non sans humour – à l'éditeur de recruter un constant externe pour auditer son code.

Les logiciels antivirus tournent avec un haut niveau de privilège sur les systèmes d'exploitation, ce qui signifie que l'exploitation d'une vulnérabilité peut donner à un attaquant un accès profond à un ordinateur. Des dizaines de sévères vulnérabilités ont été trouvé sur les 7 derniers mois dans les logiciels antivirus incluant ceux de Kaspersky Lab, Eset, Avast, AVG Technologies, Intel Security et Malwarebytes.

Réagissez à cet article

Source : *Le coffre-fort à mots de passe de Trend Micro transformé en passoire – Le Monde Informatique*

Comment l'industrie peut aussi anticiper les cyberattaques ?

Les cyberattaques se multiplient ces derniers mois et ont augmenté de 51 % (*) cette année en France, en particulier à l'encontre des technologies de l'information (messageries hackées, serveurs victimes d'attaques #DDoS entre autres). Pourtant, un tout autre domaine suscite de nouvelles préoccupations : l'industrie.
Les systèmes industriels, ou Industrial Control System (ICS), désignant l'ensemble des moyens informatisés et automatisés assurant le contrôle et le pilotage de procédés industriels, subissent les mêmes menaces que dans le milieu IT.
Cependant, une attaque à l'encontre de l'ICS peut avoir des répercussions encore plus graves, non seulement sur l'industrie en elle-même, avec son corollaire de pertes financières, mais aussi, et surtout, sur l'homme et l'environnement.

Des réseaux vulnérables, car en flux tendus
Tandis que l'IT se soucie davantage de la confidentialité des données, les industriels se préoccupent essentiellement de la disponibilité et de la rentabilité de leur production. Il faut ainsi comprendre que pour des questions de coût, il est inconcevable pour un industriel de stopper sa production, nonobstant une menace imminente.

La dernière crise ukrainienne a illustré cette problématique. Malgré des bombardements massifs, le système de production n'a pas été arrêté. Les réseaux industriels sont d'autant plus vulnérables qu'il n'est pas possible d'effectuer de maintenance sur le système, puisqu'il est en cours de production.

Mais qui sont ces « pirates » qui tirent profit de ces vulnérabilités ?
Il s'agit de groupes bien organisés, de terroristes, qui s'attaquent directement à la vulnérabilité de l'État et des grandes entreprises. On parle d'une véritable cyberarmée qui s'attaque aux réseaux industriels de plusieurs manières : déni de services, prise de contrôle à distance des systèmes, vol de données, mise en faillite par détournement de fonds, pour n'en citer que quelques-uns. En 2003, la centrale nucléaire de Davis-Besse aux USA avait été la cible d'attaques DDoS.
Pour autant, la plupart des incidents de sécurité sont accidentels, liés par exemple à l'activation fortuite de malware se trouvant dans un mail, sur une clé USB ou encore des softwares mal sécurisés.
À l'échelle de l'industrie, les attaques peuvent entraîner des retards de production, un impact économique – consécutif au vol de secrets de fabrication – une perte d'image et de contrats. In fine, l'industriel se retrouve face à une véritable perte de compétitivité.
Les réseaux industriels étant en contact direct avec la vie humaine, celle-ci est également en danger. Ces attaques peuvent en effet entraîner des accidents physiques ; l'arrêt de la production d'énergie pouvant entraîner des coupures d'électricité dans les hôpitaux qui peuvent être critiques. À plus grande ampleur, la santé humaine et l'environnement sont également menacés dans le cas d'une attaque des systèmes nucléaires.
L'exemple le plus connu est celui de Stuxnet, un ver informatique découvert en 2010 et conçu pour attaquer une cible industrielle déterminée pour l'espionner. Le ver a affecté 45 000 systèmes informatiques, y compris des ordinateurs de la centrale nucléaire de Bouchehr ainsi que 15 000 ordinateurs et centrales situés en Allemagne, en France, en Inde et en Indonésie (**).

Les industriels ne sont pas suffisamment préparés à ces types d'attaques, car les moyens mis en œuvre sont limités et la sécurité est considérée comme annexe, dans la mesure où elle n'est pas fondamentale pour assurer les services. À cela s'ajoute qu'elle représente un coût additionnel pour la production, qui se répercute sur les consommateurs qui devront payer plus cher leurs eau, électricité et autres services.
Dès lors, quelles sont les mesures pour se prémunir de ces attaques ? Quels outils peuvent être mis en place ?
La loi est un instrument essentiel pour assurer la protection des ICS et aider à recréer de la confiance. La France a mis en place, en 2006, un décret qui définit 12 secteurs d'importance vitale comprenant notamment la gestion de l'eau, la santé, l'énergie, l'alimentation et les transports, des fondamentaux pour le fonctionnement d'un État.

« Le projet de loi de programmation militaire, prévu pour 2014-2019, précise qu'il est de la responsabilité de l'État d'assurer une sécurité suffisante des systèmes critiques des OIV (opérateurs d'importance vitale). À travers quatre mesures principales, il vise à établir un socle minimum de sécurité pour les organisations.
Il donne notamment au pouvoir exécutif la possibilité d'imposer aux OIV des obligations en matière de sécurisation de leur réseau, de qualification de leurs systèmes de détection, d'information sur les attaques qu'ils peuvent subir et de soumission à des contrôles.
Avec ce texte, qui sera examiné sous peu au Sénat, l'État fixera donc des règles en collaboration étroite avec l'ANSSI. Règles que les OIV seront tenus d'appliquer, à leur frais. Les sociétés mauvaises élèves seront susceptibles de se voir infligées une sanction pouvant aller jusqu'à 750 000 euros d'amende » (***).

Au-delà de cette législation, il est essentiel, pour retarder l'attaque, de mettre un point d'honneur à la sensibilisation de l'utilisateur dans la chaîne de production, mais aussi, et surtout, de la direction des industries, en l'incitant à appliquer de bonnes pratiques au quotidien et en investissant dans les hommes et les outils (firewall, anti-vers ou encore systèmes de détection d'intrus).
Cependant, même le plus puissant des firewalls n'est pas suffisant si l'on n'identifie et ne traite pas les menaces dans le détail, sur un service en particulier. Cela sous-entend qu'il y ait un opérateur qui assure la maintenance des systèmes d'informations, sans quoi les intrusions dans les réseaux industriels ne pourront être empêchées.

(*) Source : étude réalisée par le cabinet PwC
(**) Source : Wikipédia
(***) Source : Nextimpact.com

Réagissez à cet article

Source : *Les Echos.fr – Actualité à la Une – Les Echos*