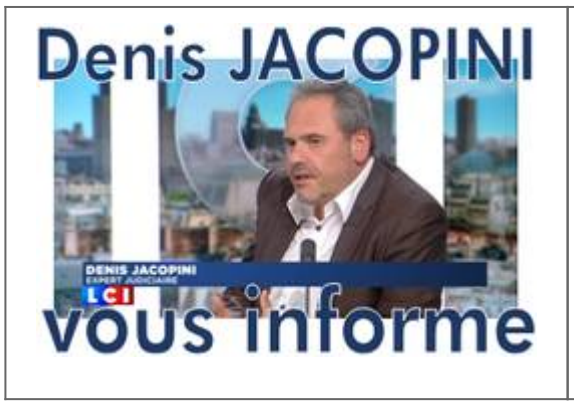
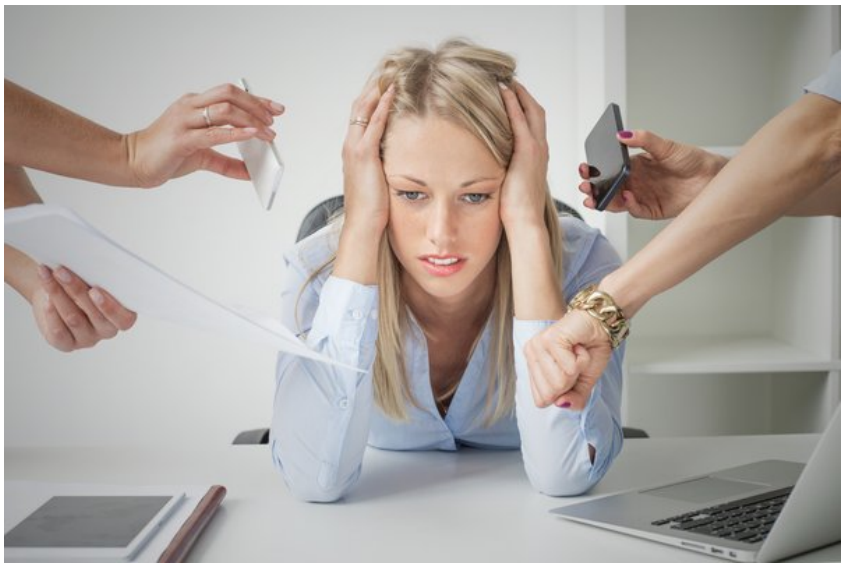
Utiliser Internet à des fins personnelles peut être un motif de licenciement



Utiliser Internet à des fins personnelles peut être un motif de licenciement

La justice européenne confirme à nouveau que dans un cercle professionnel, la direction a un droit de regard sur les échanges électroniques des salariés. Les e-mails ou autres services de communication en ligne peuvent être surveillés.



La Cour européenne des droits de l'homme (CEDH) vient de débouter un plaignant dont le licenciement avait été motivé par une utilisation indue de ressources professionnelles. Ce dernier avait utilisé à des fins personnelles, et pendant les heures de travail, des outils professionnels mais également la connexion de l'entreprise, entre autres services en ligne.
Le plaignant, un ingénieur roumain en charge des ventes, utilisait en particulier Yahoo Messenger pour converser avec des clients mais surtout avec des connaissances personnelles. La décision de la Cour met ainsi en avant le fait que l'employé échangeait très régulièrement des messages « avec son frère et sa fiancée et portant sur des questions personnelles telles que sa santé et sa vie sexuelle ».
La société a mis fin au contrat de son collaborateur au motif que son règlement intérieur interdisait l'usage de ces mêmes ressources à des fins personnelles. Cet argument a été soutenu par la justice d'autant qu'elle ne qualifie pas d'abusif le fait qu'un employeur souhaite vérifier que ses employés accomplissent leurs tâches professionnelles pendant les heures de travail.

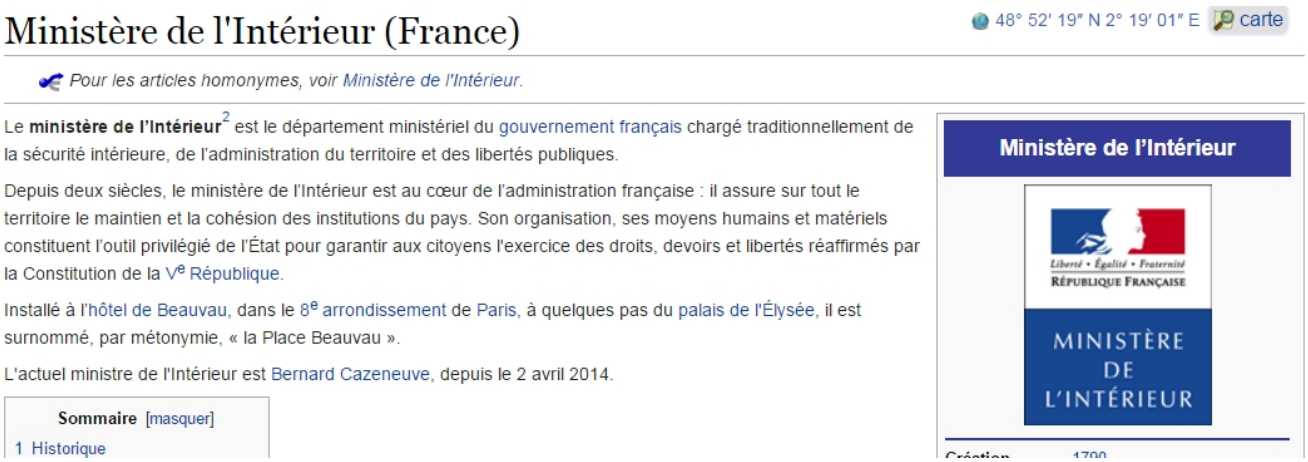
Stress travail e-mail email

La CEDH estime donc que la surveillance des communications du salarié était légitime dans la mesure où elle est considérée comme raisonnable. Cela signifie que l'employeur a cherché à préserver la productivité de ses salariés sans pour autant instaurer de politique rigide de surveillance des communications. La Cour précise que cette attention portée à l'encontre du collaborateur était organisée dans le cadre d'une procédure disciplinaire.
En France, le régime est très similaire. La justice valide régulièrement des licenciements lorsque des salariés utilisent trop souvent leurs outils informatiques pour des motifs personnels. Il est en général question de navigations régulières et conséquentes pour des tâches qui ne sont en rien en rapport avec le travail.

Réagissez à cet article

Source : *Utiliser Internet à des fins personnelles peut être un motif de licenciement*

Wikipédia bloque pour un an le ministère de l'Intérieur pour « foutage de gueule »



Ministère de l'Intérieur (France)

48° 52′ 19″ N 2° 19′ 01″ E carte

Pour les articles homonymes, voir Ministère de l'Intérieur.

Le **ministère de l'Intérieur**[2] est le département ministériel du gouvernement français chargé traditionnellement de la sécurité intérieure, de l'administration du territoire et des libertés publiques.

Depuis deux siècles, le ministère de l'Intérieur est au cœur de l'administration française : il assure sur tout le territoire le maintien et la cohésion des institutions du pays. Son organisation, ses moyens humains et matériels constituent l'outil privilégié de l'État pour garantir aux citoyens l'exercice des droits, devoirs et libertés réaffirmés par la Constitution de la Ve République.

Installé à l'hôtel de Beauvau, dans le 8e arrondissement de Paris, à quelques pas du palais de l'Élysée, il est surnommé, par métonymie, « la Place Beauvau ».

L'actuel ministre de l'Intérieur est Bernard Cazeneuve, depuis le 2 avril 2014.

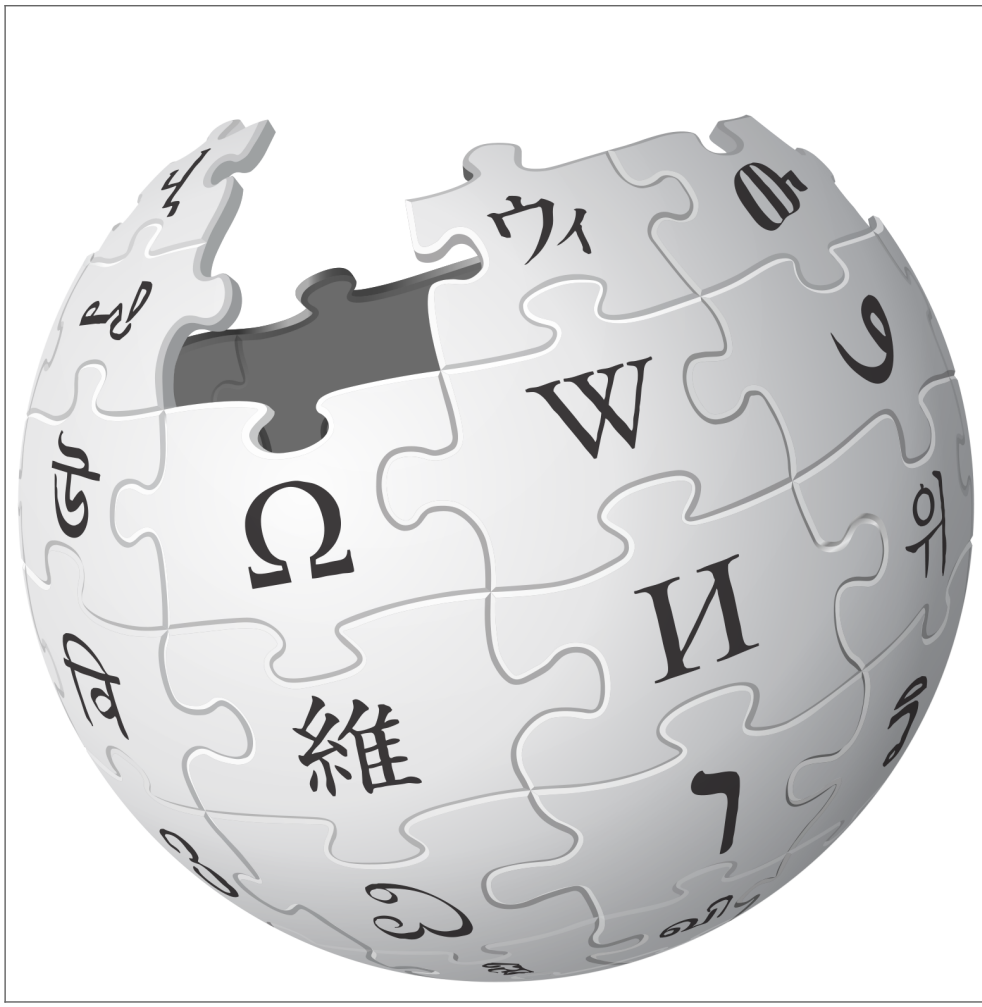
Sommaire [masquer]

1 Historique

Ministère de l'Intérieur

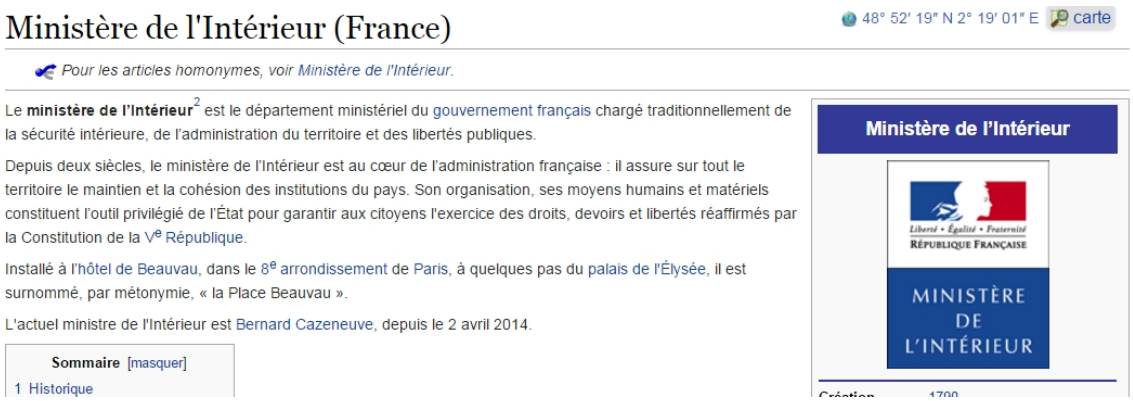
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR



Wikipédia bloqué pour un an : le ministère de l'Intérieur pour « foutage de gueule »

Le ministère de l'Intérieur a visiblement eu la main un peu lourde quant au nombre de modifications apportées sur sa page Wikipédia, mais est également accusé de différents dérapages. Résultat : un an de blocage.



Ministère de l'Intérieur (France)

48° 52′ 19″ N 2° 19′ 01″ E carte

Pour les articles homonymes, voir Ministère de l'Intérieur.

Le **ministère de l'Intérieur**[2] est le département ministériel du gouvernement français chargé traditionnellement de la sécurité intérieure, de l'administration du territoire et des libertés publiques.

Depuis deux siècles, le ministère de l'Intérieur est au cœur de l'administration française : il assure sur tout le territoire le maintien et la cohésion des institutions du pays. Son organisation, ses moyens humains et matériels constituent l'outil privilégié de l'État pour garantir aux citoyens l'exercice des droits, devoirs et libertés réaffirmés par la Constitution de la Ve République.

Installé à l'hôtel de Beauvau, dans le 8e arrondissement de Paris, à quelques pas du palais de l'Élysée, il est surnommé, par métonymie, « la Place Beauvau ».

L'actuel ministre de l'Intérieur est Bernard Cazeneuve, depuis le 2 avril 2014.

Sommaire [masquer]

1 Historique

Ministère de l'Intérieur

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR

Création 1790

Une interdiction de contribuer délivrée pour cause de « foutage de gueule ». Cela prêterait à sourire si le blocage en question ne concernait pas le ministère de l'Intérieur. D'après le Canard enchaîné, l'encyclopédie en ligne a en effet bloqué l'adresse IP de la place Beauvau pour « attitude non collaborative », « passage en force » et « foutage de gueule ».

En plus de modifications trop nombreuses à son goût, Wikipédia accuse également les fonctionnaires de vandalisme répété. Le 21 août dernier, Wikipédia a remarqué un changement sur sa page de présentation, avec la sympathique mention « Sale batar » (avec la faute). La modification émanait de l'adresse IP du ministère.

Début décembre, l'encyclopédie en ligne avait adressé un « dernier avertissement » à l'encontre du compte du ministère : visiblement, cela n'a pas suffi.

Wikipedia Beauvau

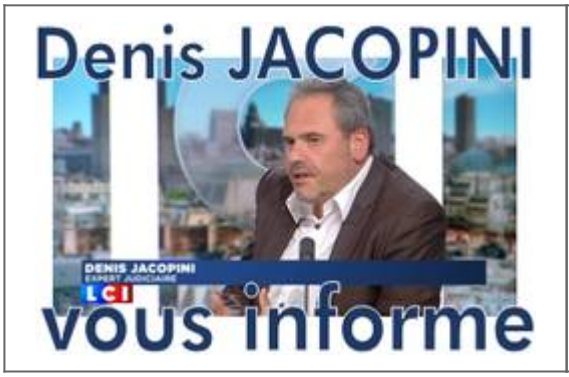
Après un premier blocage temporaire en 2013 (la fiche du préfet de police de l'époque, Bernard Boucault, avait subi six modifications en 30 minutes afin d'effacer la trace de ses démêlés avec les opposants au mariage pour tous), le compte du ministère de l'Intérieur se retrouve désormais bloqué pour un an. Difficile de comprendre comment, au sein d'un ministère, de tels agissements peuvent se répéter.

Toujours est-il qu'il y a fort à parier que ce dernier trouvera tout de même les moyens de contrôler ce qui se passe sur sa page de référence.

Réagissez à cet article

Source : *Wikipédia bloque pour un an le ministère de l'Intérieur pour « foutage de gueule »*

Amnesty critique la nouvelle loi sur la cybercriminalité au Koweït



Amnesty critique la nouvelle loi sur la cybercriminalité au Koweït

---

Amnesty International a vivement critiqué mardi une nouvelle loi sur la cybercriminalité au Koweït qui, selon cette organisation, va restreindre davantage la liberté d'expression et doit être révisée.

Le texte, qui entre en vigueur mardi, « va s'ajouter à l'éventail de lois sur le web qui restreignent déjà le droit des Koweïtiens à la liberté d'expression et doit être révisé d'urgence », écrit l'organisation de défense des droits de l'Homme dans un communiqué.
La nouvelle législation prévoit la criminalisation d'une série d'expressions en ligne comportant notamment des critiques envers le gouvernement, des dignitaires religieux ou des dirigeants étrangers, relève Amnesty.
« Cette loi répressive » fait partie d'un éventail de législations destinées à « étouffer la liberté d'expression », a commenté Saïd Boumedouha, directeur adjoint d'Amnesty International pour le Moyen-Orient et l'Afrique du nord.
Des dizaines de personnes au Koweït ont été arrêtées et poursuivies en justice, certaines servant déjà des peines de prison, en vertu d'une autre législation pour des commentaires sur les réseaux sociaux.
Votée en juin, la nouvelle loi prévoit des peines de 10 ans de prison et des amendes allant jusqu'à 165.000 dollars pour des crimes en ligne, notamment ceux liés au terrorisme.
Pour le gouvernement, cette loi est nécessaire pour combler un vide juridique et réglementer l'utilisation des services en ligne tels que Twitter.
La peine minimale en vertu de la loi consiste en six mois de prison et 6.600 dollars d'amende pour celui qui ose, illégalement, « infiltrer un ordinateur ou un réseau électronique ».
« Les autorités koweïtiennes ne doivent pas appliquer cette loi jusqu'à ce qu'elle soit révisée pour se conformer aux obligations internationales du Koweït en matière de droits de l'Homme », a dit M. Boumedouha.
« Cette loi n'appartient pas au XXIe siècle », a-t-il ajouté, soulignant que « les Koweïtiens méritent mieux » qu'une telle législation.

Réagissez à cet article

Source : *Koweït: Amnesty critique la nouvelle loi sur la cybercriminalité – Internet – Notre Temps*

Fin du support de Windows 8 – Et maintenant ?

Fin du support de Windows 8 – Et maintenant ?

Les utilisateurs de Windows 8 qui veulent continuer à bénéficier des correctifs de sécurité sur leur système d'exploitation doivent maintenant passer à la version 8.1, considérée comme le dernier service pack en date de Windows 8. Par ailleurs, comme prévu, après ce 12 janvier, Microsoft cesse également de supporter de nombreuses versions de son navigateur Internet Explorer.

A peine plus de trois ans après sa sortie en octobre 2012, le mal-aimé Windows 8 ne sera plus supporté par Microsoft au-delà ce 12 janvier 2016, date de la première mise à jour de sécurité mensuelle de l'année (le fameux Patch Tuesday, désormais appelé Update Tuesday).

Pour accéder aux prochains correctifs de sécurité apportés à l'OS – et ne pas prêter le flanc aux attaques exploitant les failles qui pourraient y être découvertes à l'avenir – les utilisateurs devront passer à Windows 8.1. Ce dernier est en fait considéré comme un « service pack » de la version 8. Or, Microsoft laisse habituellement deux ans à ses clients pour installer les services packs de ses systèmes d'exploitation et la version finale de Windows 8.1 a été livrée en octobre 2013.

Une fois passé à Windows 8.1, les utilisateurs disposeront du support standard jusqu'au 9 janvier 2018. Ils pourront ensuite accéder au support étendu jusqu'au 10 janvier 2023.

Sur son site, Microsoft décrit clairement la situation : https://support.microsoft.com/en-us/lifecycle##gp/LifeWinFAQ

Autre option, passer à Windows 10

Pour les utilisateurs de Windows 8, l'autre option est de migrer directement vers Windows 10, lancée le 29 juillet dernier. Par ailleurs, ainsi que cela avait été annoncé de longue date, le 12 janvier 2016 marque également la livraison des dernières mises à jour pour plusieurs versions du navigateur web Internet Explorer, la plupart antérieures à IE 11. Microsoft en a fourni le détail depuis longtemps dans un tableau détaillant les versions d'IE supportées pour son OS desktop, pour Windows Server et pour l'OS embarqué (Windows Embedded). On voit ainsi qu'IE 9 est toujours supporté pour Windows Vista SP2, Windows Server 2008 SP2 et IA64. Les utilisateurs de Windows 7 SP1 devront utiliser IE 11. En revanche, IE 11 ne sera plus supporté pour Windows 8 et ses utilisateurs devront passer à 8.1 Update ou 10.

Beginning January 12, 2016, only the most current version of Internet Explorer available for a supported operating system will receive technical support and security updates, as shown in the table below:

Windows Desktop Operating Systems	Internet Explorer Version
Windows Vista SP2	Internet Explorer 9
Windows 7 SP1	Internet Explorer 11
Windows 8.1 Update	Internet Explorer 11

Windows Server Operating Systems	Internet Explorer Version
Windows Server 2008 SP2	Internet Explorer 9
Windows Server 2008 IA64 (Itanium)	Internet Explorer 9
Windows Server 2008 R2 SP1	Internet Explorer 11
Windows Server 2008 R2 IA64 (Itanium)	Internet Explorer 11
Windows Server 2012	Internet Explorer 10
Windows Server 2012 R2	Internet Explorer 11

Windows Embedded Operating Systems	Internet Explorer Version
Windows Embedded for Point of Service (WEPOS)	Internet Explorer 7
Windows Embedded Standard 2009 (WES09)	Internet Explorer 8
Windows Embedded POSReady 2009	Internet Explorer 8
Windows Embedded Standard 7	Internet Explorer 11
Windows Embedded POSReady 7	Internet Explorer 11
Windows Thin PC	Internet Explorer 8
Windows Embedded 8 Standard	Internet Explorer 10
Windows 8.1 Industry Update	Internet Explorer 11

For customers running on an older version of Internet Explorer, such as Internet Explorer 8 on Windows 7 Service Pack 1 (SP1), Microsoft recommends customers plan to migrate to one of the above supported operating systems and browser combinations by January 12, 2016.

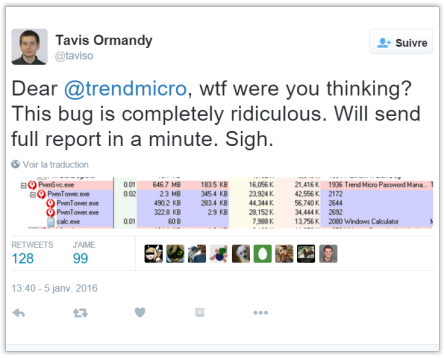
Réagissez à cet article

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*

Algorithmes prédictifs et Big Data

Algorithmes prédictifs et Big Data

Savoir ce que sera demain, ce mythe philosophique personnalisé par Cassandre dans l'antiquité Grecque est-il aujourd'hui en passe de devenir une réalité scientifique ?

Nombreuses sont les applications qui aujourd'hui s'appuient sur des algorithmes prédictifs, que ce soient dans les domaines du marketing, de la finance ou encore de la santé. Cet engouement multidisciplinaire est le résultat d'un phénomène, qui naquit il y a plus de 10 ans mais qui a aujourd'hui trouvé un terreau favorable de croissance : le Big Data.

Socle de cette émergence, la donnée constitue un or noir disponible, aisée d'exploitation de prime abord mais aussi potentiellement facteur décisionnel dans certaines disciplines. Au cours des dernières années est apparu le terme de «données massives» pour englober la mine de renseignements collectée à partir de nos activités quotidiennes, des articles publiés, de nos interactions sociales et des objets de plus en plus connectés, c'est à dire eux même générateurs de données.
La donnée offre la possibilité d'envisager des évolutions à court, moyen et long termes comme des comportements à venir parfois même en temps réel. Elle permet de faire le grand écart entre la globalisation et l'individualisation. En effet, il est, à la fois, possible de suivre et d'anticiper les grandes épidémies à l'échelle mondiale tout en analysant le comportement individuel de monsieur X par rapport à ses déplacements ou ses achats.
La lutte contre la criminalité n'échappe pas à l'intérêt que présente la donnée dans la capacité à prévoir les évolutions et pourquoi pas le comportement criminel. En effet, les données massives constituent la source de l'analyse prédictive en ce qu'elles alimentent des applications à vocation opérationnelle.
Derrière la notion simplificatrice et vulgarisée d'algorithme prédictif se dissimule un processus analytique complexe et polyvalent. Loin d'être le fruit d'une génération spontanée, l'analyse prédictive repose sur des préceptes mathématiques et statistiques à des fins d'extraction de connaissances et de formes criminelles particulières. Il n'existe pas de logiciels ou d'algorithmes miracles pour lutter contre la délinquance. Il s'agit de développer des méthodes, de les tester, de les évaluer préalablement à une quelconque utilisation. Les méthodes reposent sur des techniques d'apprentissage capable d'exploiter les données dans leurs multiples dimensions. Loin de toute notion de préemption, l'analyse prédictive a une vocation de prévention, c'est à dire non pas d'agir préalablement à toute commission d'infraction mais plutôt d'interrompre l'évolution d'un processus en cours. A l'opposé des clichés véhiculés par la fiction (Minority Report, Person of Interest), l'analyse prédictive constitue une aide à la décision pour un chef opérationnel qui la complète par une approche prospective. En effet, l'anticipation criminelle nécessite de prendre en compte l'héritage des événements du passé, c'est la prédiction. Mais elle intègre aussi, en élaborant les scenarii les plus probables, des événements ponctuels impactant le futur, c'est le domaine de la prospective. Dès lors, en matière de lutte contre la criminalité, le pilotage ne peut s'effectuer par la donnée comme cela peut être le cas dans d'autres disciplines. En effet, l'analyse prédictive apporte des éléments objectifs de compréhension mais quoiqu'il arrive et en dépit de la masse de données disponible, incomplets. Elle est, par exemple, utilisée dans la prise en compte des perspectives d'évolution d'infractions de masse telles que les cambriolages. Elle peut aussi être utilisée dans la détection préalable de fraudes sociales ou bancaires ou encore dans la compréhension à des fins d'anticipation des variables pesant sur certaines formes d'infractions. En effet, la politique d'ouverture et de partage des données publiques permet de tirer profit de variables liées à un contexte social ou économique ou encore à l'évolution météorologique, voire à la création de nouvelles infrastructures.
En dépit de l'intérêt manifeste que présentent les méthodes prédictives, il convient de se garder de tout risque d'atteintes aux libertés individuelles. Ce point est un préalable obligatoire à un quelconque déploiement en matière de sécurité publique où la donnée à caractère personnel est exclue du champ d'analyse. Outre cette question essentielle, le risque de l'analyse prédictive est aussi une mauvaise interprétation de ce qu'est réellement l'apport de la prédiction. Gardons nous du joug infligé par Apollon à Cassandre.

Réagissez à cet article

Source : *L'algorithme prédictif [par Patrick PERROT, Chef de la Division Analyse et Investigations Criminelles, Service Central de Renseignement Criminel de la Gendarmerie Nationale] | Observatoire FIC*

Comment l’industrie peut aussi anticiper les cyberattaques ?

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

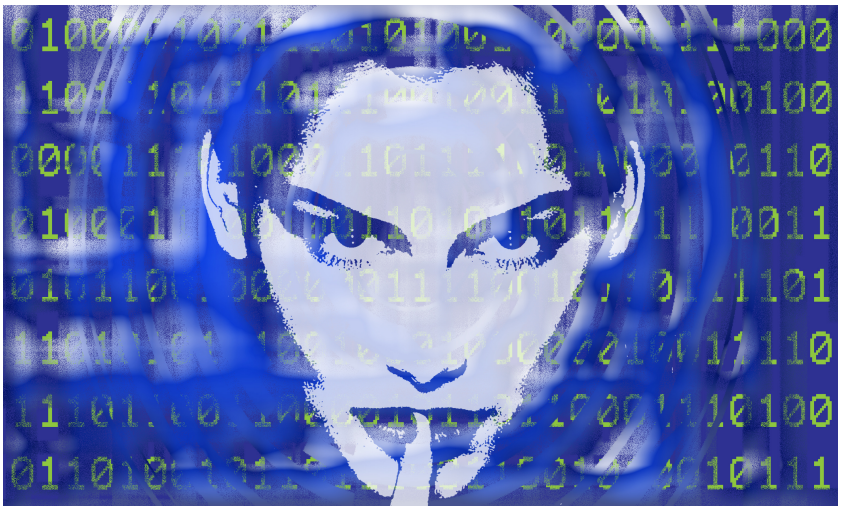
Réagissez à cet article

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

Antivirus software could make your company more vulnerable

	Antivirus software could make your company more vulnerable !

Security researchers are worried that critical vulnerabilities in antivirus products are too easy to find and exploit



Imagine getting a call from your company's IT department telling you your workstation has been compromised and you should stop what you're doing immediately.
You're stumped: You went through the company's security training and you're sure you didn't open any suspicious email attachments or click on any bad links; you know that your company has a solid patching policy and the software on your computer is up to date; you're also not the type of employee who visits non-work-related websites while on the job. So, how did this happen?

A few days later, an unexpected answer comes down from the security firm that your company hired to investigate the incident: Hackers got in by exploiting a flaw in the corporate antivirus program installed on your computer, the same program that's supposed to protect it from attacks. And all it took was for attackers to send you an email message that you didn't even open.
This scenario might sound far-fetched, but it's not. According to vulnerability researchers who have analyzed antivirus programs in the past, such attacks are quite likely, and may already have occurred. Some of them have tried to sound the alarm about the ease of finding and exploiting critical flaws in endpoint antivirus products for years.
Since June, researchers have found and reported several dozen serious flaws in antivirus products from vendors such as Kaspersky Lab, ESET, Avast, AVG Technologies, Intel Security (formerly McAfee) and Malwarebytes. Many of those vulnerabilities would have allowed attackers to remotely execute malicious code on computers, to abuse the functionality of the antivirus products themselves, to gain higher privileges on compromised systems and even to defeat the anti-exploitation defenses of third-party applications.
Exploiting some of those vulnerabilities required no user interaction and could have allowed the creation of computer worms – self-propagating malware programs. In many cases, attackers would have only needed to send specially crafted email messages to potential victims, to inject malicious code into legitimate websites visited by them, or to plug in USB drives with malformed files into their computers.

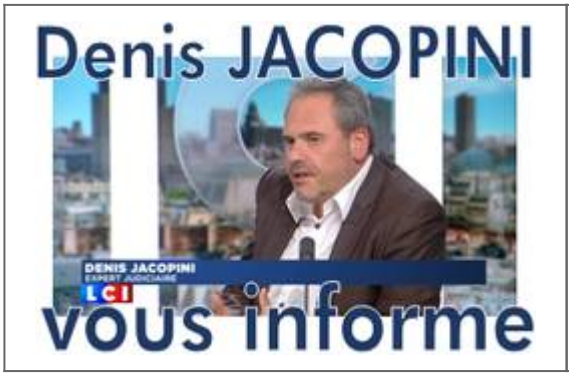
Attacks on the horizon

Evidence suggests that attacks against antivirus products, especially in corporate environments, are both possible and likely. Some researchers believe that such attacks have already occurred, even though antivirus vendors might not be aware of them because of the very small number of victims.
The intelligence agencies of various governments have long had an interest in antivirus flaws. News website The Intercept reported in June that the U.K. Government Communications Headquarters (GCHQ) filed requests in 2008 to renew a warrant that would have allowed the agency to reverse engineer antivirus products from Kaspersky Lab to find weaknesses. The U.S. National Security Agency also studied antivirus products to bypass their detection, according to secret files leaked by former NSA contractor Edward Snowden, the website said.

Réagissez à cet article

Source : *Antivirus software could make your company more vulnerable | Computerworld*

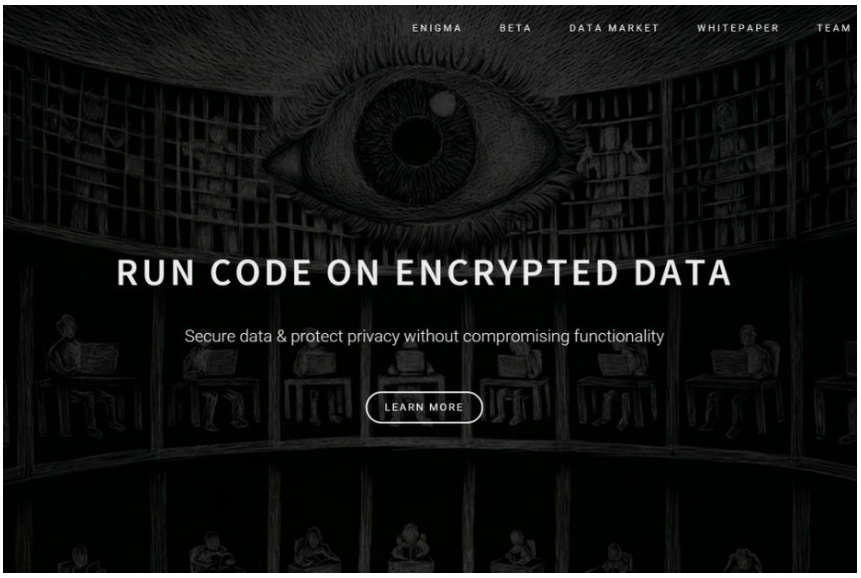
Enigma, le système de cryptage de données basé sur le blockchain du MIT Media Lab



Enigma, le système de cryptage de données basé sur le blockchain du MIT Media Lab

---

Avec Enigma, système de cryptage de données basé sur le blockchain, des informations confidentielles peuvent être stockées et partagées en ligne, sans intervention d'un tiers de confiance pour contrôler leur utilisation.



Enigma. Derrière ce nom mystérieux se cache l'une des dernières créations du MIT Media Lab, l'un des laboratoires de recherche du Massachusetts Institute of Technology. Ce système de cryptage de données est basé sur le blockchain, la technologie qui sous-tend le bitcoin (monnaie virtuelle mise en circulation en 2009). Elle fonctionne grâce au partage d'un registre d'informations par l'ensemble d'une communauté d'internautes.

Enigma, dont la version bêta sera lancée prochainement, permettra à des utilisateurs anonymes (particuliers, entreprises, associations…) de stocker dans le cloud et de partager des informations sensibles avec des tiers, de manière sécurisée. Pas besoin d'un intermédiaire de confiance, qui aurait accès à ces data pour contrôler leur utilisation et les crypter. Ces opérations sont effectuées par un réseau d'ordinateurs membres, grâce au système du blockchain. Les informations peuvent être traitées par des algorithmes, sans que le jeu de données brut ne soit jamais révélé dans sa totalité à l'une des parties.

DES RETOMBÉES DANS LE DOMAINE DU MACHINE LEARNING

Le registre blockchain, partagé par les ordinateurs membres du réseau, contrôle l'identité des utilisateurs d'Enigma (via un code, car ils sont anonymes) et leur donne accès ou non à tout ou partie des données. Il enregistre l'ensemble des opérations réalisées sur Enigma : enregistrement de nouvelles informations, consultation, opérations réalisées sur ces data…

Les données stockées par Enigma pourront être analysées par des applications et des logiciels extérieurs, tout en maintenant ces informations sous le contrôle de leur propriétaire. Le programme pourrait avoir des retombées intéressantes dans le domaine de la data science et du machine learning.

UN NOM DE BAPTÊME HISTORIQUE

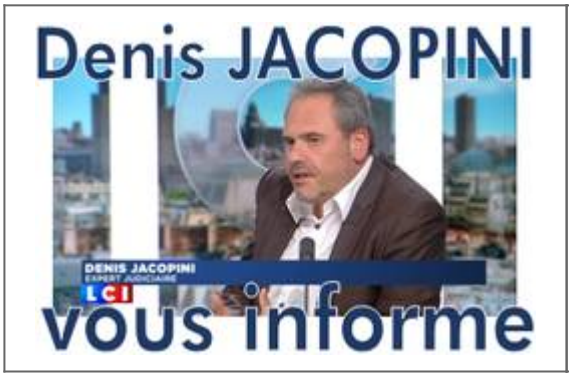
Enigma pourrait également contribuer au développement d'un Internet des objets respectueux de la vie privée de ses utilisateurs, souligne le site spécialisé Bitcoin Magazine dans un article présentant le projet. Les propriétaires des données pourront, s'ils le souhaitent, les monétiser. Ils pourraient par exemple vendre à des laboratoires pharmaceutiques qui réalisent des recherches un accès partiel et contrôlé à leurs données de santé.

Guy Zyskind, étudiant au MIT, et Oz Nathan, entrepreneur qui a travaillé par le passé avec la défense israélienne, sont à l'origine de ce programme. Ils n'ont pas choisi son nom par hasard. Le système de cryptographie électro-mécanique utilisé par les Allemand pendant la deuxième guerre mondiale était baptisé Enigma. Un groupe de chercheurs, dont faisait notamment partie Alain Turing, a réussi à trouver la clef de ce code complexe.

Réagissez à cet article

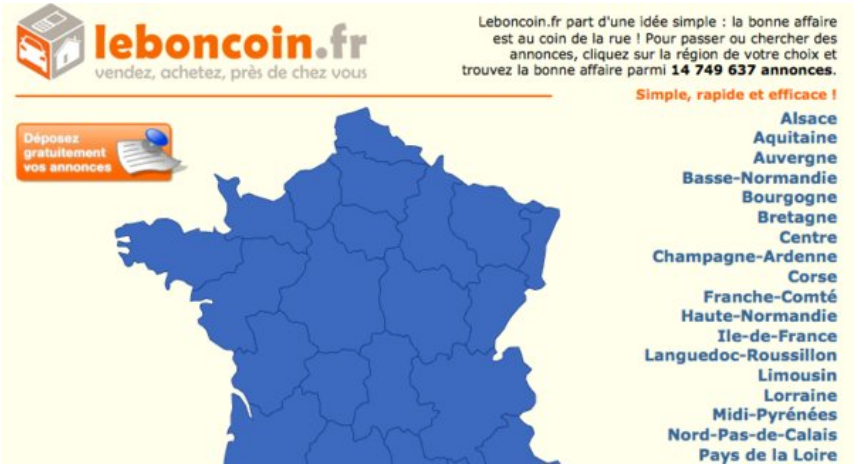
Source : *Enigma, le système de cryptage de données basé sur le blockchain du MIT Media Lab*

Plusieurs escrocs sur Leboncoin écopent de peines de prison



Plusieurs escrocs sur Leboncoin écopent de peines de prison

Les autorités utilisent Leboncoin pour surveiller les escrocs qui revendent du matériel volé. Plusieurs forces de police indiquent avoir réussi à arrêter des auteurs présumés, certains ont même été condamnés à des peines de prison.



Comme bon nombre de plates-formes de vente en ligne, Leboncoin.fr peut servir pour des escrocs de moyen d'écouler une marchandise indûment obtenue voire d'appâter des victimes. En région parisienne, un groupe de personnes vient d'être condamné à des peines de prison pour avoir revendu des voitures sur le site.
Ces véhicules d'occasion étaient achetés avec de faux chèques de banque pour les revendre, 30 à 40 % moins cher que l'argus, contre des espèces. Des annonces étaient régulièrement publiées sur Leboncoin puis rapidement retirées, une fois la vente conclue. Au total, 71 automobiles ont été répertoriées par les forces de police.
Selon Le Parisien, les escrocs ont pu être repérés notamment grâce aux annonces publiées sur le site.
Le cerveau du réseau, un homme de 28 ans, écope d'une peine de 5 années de prison dont 1 an avec sursis avec mise à l'épreuve. Il devra en outre rembourser les victimes. Les autres membres ont été condamnés par le tribunal correctionnel de Pontoise à 4 et 2 ans de prison (associées à des peines de sursis).

Le site internet leboncoin.fr
Un voleur arrêté après avoir mis des annonces sur Leboncoin
En Bretagne, les autorités indiquent avoir interpellé un homme soupçonné d'avoir dérobé du matériel de jardinage auprès d'une enseigne locale. L'individu a volé des objets pour un préjudice total estimé à 2 500 euros puis a tenté de revendre une partie du butin sur Leboncoin, sans se soucier que le vendeur ou la gendarmerie surveillerait la plate-forme.
Dans les jours suivants le délit, le responsable du magasin qui avait subi le vol a trouvé une annonce pertinente. « Nous avons ensuite travaillé à partir de cette annonce, puis nous sommes remontés jusqu'à l'auteur présumé des cambriolages », explique le maréchal des logis-chef Goby auprès du quotidien Ouest-France.
Le domicile de la personne a été perquisitionné et nombre d'objets dérobés s'y trouvaient. L'affaire a été transmise au parquet de Brest, où sera jugé l'auteur présumé.

Réagissez à cet article

Source : *Plusieurs escrocs sur Leboncoin écopent de peines de prison*