

# Confidentialité et cryptage récompensés

✕	<b>Confidentialité et cryptage récompensés</b>
<b>Sophia Genetics. La société lausannoise devient la première entreprise doublement certifiée ISO 13485 et ISO 27001.</b>	
<small>Sophia Genetics, leader européen en génomique clinique et séquençage ADN de nouvelle génération (NGS), devient la première entreprise doublement certifiée ISO 13485 et ISO 27001.</small>	
<small>D'après un communiqué, l'entreprise précise que les certifications du groupe BSI récompensent, entre autres, l'approche de Sophia Genetics du traitement de l'information et du cryptage des données de patients. Cette dernière, en instance d'obtention de brevet, vise à protéger la confidentialité des informations génomiques.</small>	
<small>Les serveurs redondants installés par Sophia Genetics dans divers sites hautement sécurisés, offrent à ses clients la confiance nécessaire afin de traiter, analyser et stocker les données de milliers de patients suspectés ou atteints de maladies chroniques.</small>	
<small>La certification ISO 27001 a été attribuée à la plateforme Information Security Management System de Sophia pour toutes les informations sécurisées internes et externes de ses clients.</small>	
<small>Sophia Genetics se charge à l'heure actuelle de l'analyse, du stockage et du traitement des données de plus de 30 hôpitaux et laboratoires de pointe en Europe.</small>	
<small>Après cette lecture, quel est votre avis ?</small>	
<small>Cliquez et laissez-nous un commentaire...</small>	
<small>S o u r c e</small>	
<small><a href="http://www.agefi.com/une/detail/archive/2014/december/artikel/sophia-genetics-la-societe-lausannoise-devient-la-premiere-entreprise-doublement-certifiee-iso-13485-et-iso-27001-388417.html">http://www.agefi.com/une/detail/archive/2014/december/artikel/sophia-genetics-la-societe-lausannoise-devient-la-premiere-entreprise-doublement-certifiee-iso-13485-et-iso-27001-388417.html</a></small>	

---

# Le site web de l'Internet System Consortium touché par un malware

✕	<b>Le site web de l'Internet System Consortium touché par un malware</b>
---	--

Le site web de l'Internet System Consortium, qui édite notamment la solution BIND pour la gestion de DNS, a été victime d'un malware. Les utilisateurs qui ont visité le site web de l'ISC dans les dernières semaines sont invités à scanner leurs machines.

Le site web de l'Internet System Consortium a été temporairement mis hors ligne suite à la découverte d'une attaque ayant pu affecter les visiteurs du site. Une page statique est actuellement en ligne avec des indications nécessaires pour les utilisateurs de BIND, le serveur DNS proposé par l'ISC. L'attaque subie par le consortium n'a pas affecté les programmes publiés par l'ISC dont le code source est hébergé sur un serveur différent du site web. Selon The Register, qui a contacté un membre de l'Internet System Consortium, l'attaque n'était pas ciblée et n'a touché que le site web, qui avait recours au CMS WordPress. Une attaque automatisée « inhérente aux CMS de ce type » ajoute Dan Mahoney, responsable de la sécurité de l'ISC.

L'attaque a permis aux attaquants de rediriger certains internautes vers une page distribuant un malware windows, le Angler Exploit Kit. Celui-ci est connu depuis quelques temps et exploite plusieurs failles dans Flash, Internet Explorer et SilverLight pour ensuite exécuter du code malveillant sur la machine ciblée. La finalité du malware reste encore peu connue, mais mieux vaut prévenir que guérir. Pour l'instant, l'ISC n'a pas encore signalé d'utilisateur infecté par leur site mais a préféré mettre le site hors ligne en attendant de résoudre le problème.

Plus de peur que de mal donc, mais l'ISC fait partie des sociétés vitales pour Internet : le consortium développe et maintient le code de BIND, le serveur DNS le plus largement utilisé aujourd'hui sur le réseau et héberge l'un des 13 serveurs racine du DNS. Si ces derniers ne sont pas affectés par l'attaque, les internautes et administrateurs systèmes qui ont visité le site wordpress de l'ISC avant le 22 décembre ont en revanche de quoi s'inquiéter.

Après cette lecture, quel est votre avis ?  
Cliquez et laissez-nous un commentaire...

Source : <http://www.zdnet.fr/actualites/le-site-web-de-l-internet-system-consortium-touche-par-un-malware-39812011.htm>  
Par Louis Adam

# Attention à bien déclarer à la CNIL le traitement de vos fichiers clients, salariés, patients...



Attention à bien déclarer à la CNIL le traitement de vos fichiers clients, salariés, patients...

S'il n'a pas été déclaré à la CNIL, votre traitement de données personnelles est illicite. Tout comme les éléments qu'il vous fournira pour justifier le licenciement d'un salarié.

Tout traitement de données personnelles est illicite s'il n'a pas été préalablement et correctement déclaré à la Cnil (sauf si ces moyens de traitement sont couverts par l'une des 19 dispenses prononcées par la commission). Conséquence : la chambre sociale de la Cour de Cassation a cassé l'arrêt de la Cour d'Appel de Douai, qui avait approuvé le licenciement d'une salariée pour cause réelle et sérieuse alors que ce dernier était fondé uniquement sur le système de contrôle du nombre et du contenu des courriels des salariés mis en place par la société.



Cette dernière n'ayant pas déclaré ce système (qui constitue un traitement de données personnelles) auprès de la Cnil, ce système était illégal et la société ne pouvait donc pas utiliser les preuves qu'elle s'était ainsi constituées. Il convient de rappeler que la déclaration auprès de la Cnil n'est pas la seule condition de la légalité d'un traitement de données personnelles, cette légalité étant également conditionnée, en particulier, par l'information préalable des personnes concernées.

Non respect de la Loi Informatique et Libertés du 6 janvier 1978 :  
Peines encourues : 5 ans de prison et 300 000 euros d'amende

Articles sur le même thème :

Se mettre en conformité avec la CNIL – Oui mais comment ?

Est-ce que votre site Internet est en règle avec la CNIL ?

Après cette lecture, quel est votre avis ?  
Cliquez et laissez-nous un commentaire...

Source

<http://www.chefdentreprise.com/Thematique/management-rh-1026/droit-social-10119/Breves/Jurisprudence-Attention-declarer-CNIL-votre-systeme-contrôle-donnees-personnelles-248669.htm>

# Sony adopte de nouvelles règles de sécurité – PS4, PS3, PS Vita News – Play3-Live



Sony adopte de nouvelles règles de sécurité

Comme nous avons pu le voir depuis quelques jours, ni Sony, ni Microsoft ne sont à l'abri d'action malveillante de la part d'un certains groupe d'individus mal intentionné. Suite aux différents hacks dont il fut victime récemment, Sony se rend compte qu'une protection en ligne appropriée est nécessaire pour garder les clients et les parties prenantes heureuses, ils sont donc dans l'optique d'une embauche d'un nouveau directeur du management d'ingénierie en vulnérabilité pour prévenir d'autres incidents.

L'offre d'emploi stipule que le candidat retenu sera responsable de ce qui suit:

- Unifier et améliorer l'architecture de sécurité mondiale du groupe, inclure une stratégie de gestion de la vulnérabilité cohérente englobant toutes les sociétés du groupe Sony
- Servir en tant qu'expert technique référent en matière de sécurité et conseiller pour les initiatives prioritaires de sécurité
- Gérer les équipes d'ingénieurs et développeurs hautement qualifiés, conduire et orienter la pensée, le développement de carrière, le mentorat et les conseils techniques
- Superviser l'élaboration de systèmes de gestion de la vulnérabilité, des initiatives, intégration et l'assistance d'évaluation technique
- Diriger des équipes et coordonner les efforts ou initiatives concernant les tests de pénétration, le système et la gestion de la vulnérabilité de l'application, l'évaluation globale des risques techniques, et les opérations de chasse
- Développer et affiner des normes techniques de sécurité de l'information, des directives et de la formation
- Soutenir la coordination des activités de planification budgétaire de l'entreprise liées à des outils d'information et de services de sécurité, afin d'inclure le leadership des activités de planification d'entreprise de milieu de gamme
- Appuyer la gestion, la planification et l'exécution du budget de l'ingénierie de la sécurité mondiale
- Assembler et entraîner divers ensembles de l'information et des intervenants experts sécurité dans la formulation des exigences de sécurité de l'information unifiée et des normes d'architecture pour la plupart des projets et contrats du groupe
- Servir en tant qu'expert en la matière fournissant des services consultatifs intra-entreprise liés à la stratégie de l'architecture de sécurité et de mise en œuvre de la technologie

Vous l'aurez compris, Sony semble apprendre de ses erreurs et chercher une pointure dans le domaine de la sécurité afin de ne plus être victime des soucis rencontrés il y a quelques heures encore.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire..

Source : <http://www.play3-live.com/news/sony-adopte-de-nouvelle-reegles-de-securitees-70376>

---

# DDoS du PSN – Nous avons discuté avec un membre de Lizard Squad



DDoS du PSN – Nous avons discuté avec un membre de Lizard Squad

Après trois jours de coupure, de connexion impossible et d'erreur de maintenance, le PSN semble, ce matin, plutôt accessible pour la plupart des joueurs autant sur PS4 que PS3 et PS Vita. Hier, dans la soirée, un membre de Lizard Squad a souhaité rentrer en contact avec nous, pour nous proposer quelques informations. Nous avons donc pu discuter par message écrit avec @AironeHD, qui nous en dit plus sur les causes du DDoS du PSN de Sony, et la durée souhaitée des coupures de ce même PSN.

#### **Lizard Squad veut montrer l'incompétence de Sony**

Ce qui ressort de notre interview avec l'un des contributeurs français de Lizard Squad est que le groupe de hacker ne souhaite pas faire de mal aux joueurs. Non, la motivation est de prouver que Sony est incompétent dans sa gestion du PSN : « Nous ne sommes pas méchants nous voulons simplement « troller » ces chefs incompétents, incapables de protéger des serveurs alors qu'ils ont les moyens financiers pour le faire. » Nous apprenons également au cours de l'interview que le souhait premier de Lizard Squad n'est pas de pirater les comptes PSN et Xbox Live pour récupérer des données personnelles et bancaires, mais simplement de bloquer les serveurs online.

Lorsque nous avons demandé à AironeHD quel était le motif des attaques, celui-ci nous a répondu : « Montrer tout simplement aux chefs de Sony (avant, Microsoft également, mais plus maintenant) que leurs systèmes de sécurité sont faibles. Et que tout le monde (informaticien assez doué) peut rentrer dans leurs systèmes. Et que l'on soit connus pour nos actes. »

#### **Le PSN sera perturbé tant que Sony ignorera Lizard Squad**

Nous avons ensuite demandé à AironeHD combien de temps allait durer les coupures régulières du PSN. La réponse est claire et non équivoque : « C'est une durée indéterminée, impossible de vous dire pour l'instant. On ne compte pas lâcher. Les chefs de Sony essayent de nous ignorer. Alors nous continuons. » Enfin, nous avons tenté de savoir pourquoi le Xbox Live était moins perturbé que le PSN. Le membre de Lizard Squad déclare vaguement que les attaques échoueraient assez souvent, et qu'il était donc plus compliqué de mettre à terre le Xbox Live que le PSN. Pour les indisponibilités des serveurs EA et Activision (FIFA et Call of Duty: Advanced Warfare), les actes de Lizard Squad sont simplement du « troll » selon AironeHD.

N.B – Cette interview avec un membre présumé de Lizard Squad en France est à but uniquement informative. Tout comme les autres membres du groupe de hacker sur Twitter, nous ne pouvons pas prouver l'implication de AironeHD dans les attaques DDoS du PSN via des pièces justificatives. Ces déclarations ne sont donc pas des preuves, mais un bon aperçu de ce que souhaite vraiment faire Lizard Squad. Merci de votre compréhension.

Après cette lecture, quel est votre avis ?

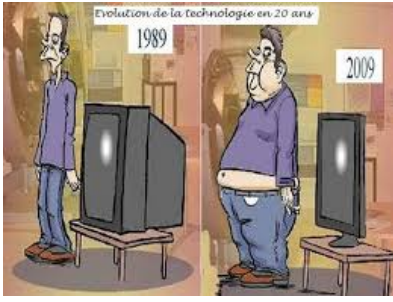
Cliquez et laissez-nous un commentaire...

Source

<http://playerone.tv/news/v/6352/ddos-du-psn-nous-avons-discut%C3%A9-avec-un-membre-de-lizard-squad.html>

---

# L'évolution des technologies inquiète...



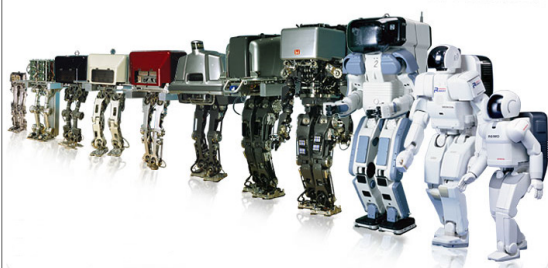
L'évolution  
des technologies inquiète...

**56% des répondants à l'enquête mondiale Global Evolving Workforce menée par TNS pensent que la technologie évolue trop rapidement et qu'elle aura un impact négatif sur eux. Ils s'attendent à une automatisation des tâches et craignent que le big data n'entrave leur liberté individuelle.**

Si les utilisateurs sont persuadés que leurs smartphones, tablettes, PC portables et autres équipements informatiques les rendent plus productifs au bureau, ils s'inquiètent du rôle croissant de la technologie dans leur vie privée. Selon les résultats de l'étude Global Evolving Workforce menée auprès de 4764 employés dans une dizaine de pays, dont la France, 56% des sondés pensent en effet que la technologie a un effet néfaste sur eux. Les auteurs de ce rapport réalisé par le cabinet TNS pour le compte d'Intel et de Dell entre le 11 juillet et le 5 septembre dernier, ont indiqué que ces « downsiders » de la technologie estimaient que sa prolifération contribuait à la fois à les séparer et à les rendre moins importants. Ils pensent également que la technologie évolue trop rapidement et qu'ils ne peuvent plus suivre. Outre des doutes sur la responsabilité des entreprises à l'égard de leurs données personnelles, ils craignent que la tendance des big data se traduise par la fin de leur liberté individuelle.

Toutefois, certains s'attendent à ce que les big data soient utilisées à des fins de promotions internes ou d'évolution de carrière. De leur côté, près de 40% pensent que les recrutements seront effectués par des logiciels entièrement automatisés, plutôt que par des humains. Certains redoutent également d'être surveillés par des webcams lorsqu'ils travaillent chez eux. L'étude précise que les « downsiders » constituent la majorité des personnes interrogées dans des pays développés comme les États-Unis, Royaume-Uni, le Japon et la France, pays où la technologie est fortement implantée dans les entreprises. A l'opposé, les « upsiders » seraient majoritaires dans les pays émergents, comme la Chine, l'Inde et les Émirats arabes unis, l'IT faisant partie des habitudes de vie depuis moins longtemps.

**Des évolutions graduelles plutôt que des bouleversements**  
Les upsiders (44% du total mondial) estiment pour leur part que la plupart des problèmes peuvent être résolus grâce à la technologie, et que celle-ci contribue à les rassembler. Pour eux, l'IT est un facteur clé qui améliore leur existence et sans elle, ils ne seraient pas heureux. Les auteurs du rapport pensent qu'avec le temps, on pourra déterminer qui des deux groupes a raison mais ils s'attendent à ce que la réponse soit à la fois valable pour l'un et l'autre. Si l'on se penche sur les résultats obtenus par pays, 66% des répondants basés aux États-Unis considèrent que la technologie finira par atteindre une limite dans sa capacité à améliorer leur productivité, mais que cela n'arrivera pas tout de suite. Un peu moins d'un quart pensent que leurs emplois seront entièrement automatisés, tandis que sept sur dix jugent qu'il est préférable de faire réaliser certaines tâches par des humains. En Chine, ils ne sont que 46% à penser la même chose.



En clair, ces actifs sont convaincus des gains de productivité résultant de la technologie et ils pressentent des changements graduels plutôt que des perturbations. 87% pensent que les tablettes remplaceront les PC (même si aucune date n'a été avancée), tandis que 92% estiment que la reconnaissance vocale finira par se substituer au clavier. « Je considère que ces personnes sont l'épine dorsale du travail réalisé et qu'ils vont incroyablement gagner en importance aujourd'hui et à l'avenir », a déclaré Steve Lalla, vice-président et responsable du cloud chez Dell. « Ce qui se passe, c'est que les collaborateurs souhaitent se rapprocher des clients », a-t-il ajouté. « Pour cela, ils doivent être mobiles et aller par monts et par vaux. La technologie permet de faciliter les choses, mais elle ne peut pas nécessairement tout faire. »

**Une perception du télétravail qui diverge selon les pays**



L'enquête Evolving Workforce menée par TNS a également dressé un état des lieux des tendances en matière d'habitudes de travail. 52% des répondants jugent que ceux qui sont habitués à travailler chez eux sont au moins autant productifs que s'ils travaillaient au bureau, 29% n'ayant pas d'opinion tranchée. Aux États-Unis, 40% jugent la productivité à domicile supérieure à celle au bureau, tandis qu'en Chine, cette part s'élève à 50%. Chez Dell, 20% des 100 000 collaborateurs du groupe font partie d'un programme de travail flexible, une proportion qui devrait atteindre 50% en 2020. La compagnie estime que cette pratique améliore la productivité de ses équipes.

Dans ses enquêtes internes, le groupe a constaté une augmentation de la satisfaction de ses salariés due à la mise en place du télétravail. De plus, la collaboration à distance lui aurait permis d'économiser 12 M\$ et d'éviter 6 700 tonnes d'émissions de gaz à effet de serre.

L'enquête note en parallèle un écart important entre les pays sur les attitudes des entreprises envers le télétravail. Ainsi, l'Allemagne et le Japon ont une culture traditionnellement ancrée sur le travail réalisé au sein de l'entreprise. En France et en Allemagne, certains employeurs ont décidé de désactiver leurs plates-formes de messagerie durant les week-ends pour réduire la charge de travail de leurs employés. Dans le même temps, certains collaborateurs sont mieux équipés chez eux qu'au bureau et ont des accès plus rapides à Internet, « De ce fait, la pratique du travail est plus répandue qu'auparavant », a conclu Bob O'Donnell, fondateur de Technalysis Research.

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs aux **risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

Après cette lecture, quel est votre avis ?  
Cliquez et laissez-nous un commentaire...

Source : <http://www.lemondeinformatique.fr/actualites/lire-les-salaries-des-pays-developpes-inquiets-face-aux-nouvelles-technologies-59598.html>

Article de Véronique Arène avec IDG NS

Personnalisation : Denis JACOPINI

---

# Au Japon, une banque de visages de clients suspectés de vols à l'étalage



Au Japon, une banque de visages de clients suspectés de vols à l'étalage

## Reconnaissance faciale des boutiques en réseau

**Au Japon, un réseau de magasins se partagent une banque de visages de clients suspectés de vols à l'étalage ou de ceux qui « créent » des problèmes. Ceci sans que les personnes concernées en aient connaissance.**

Automatically recorded images of shoppers' faces taken by security cameras have been shared among 115 Japanese supermarkets and convenience stores as an anti-shoplifting measure, without customers' knowledge.

Although the images are used mainly to prevent shoplifting, experts and industry bodies say it is necessary to make clear rules because providing people's facial data to a third party could constitute an invasion of privacy.

The facial data in question was shared by 115 stores of 50 separate operators that have installed a shoplifting prevention system that a Nagoya-based software development company had started marketing in October of last year.

The stores include major convenience stores operated by individuals under franchise contracts. At these shops, security cameras film all customers' faces. If a person shoplifts or makes an unreasonable complaint at one of the stores, security camera footage of the person is processed into facial data with the recognition system and classified into categories such as « shoplifter » and « complainer ».

They are then sent to the software firm's server to be recorded. The facial images themselves, however, cannot be browsed from other stores.

Once registered on the digital blacklist, however, a warning is issued to the staff of other stores – in a way only the staff can notice – when the face-recognition system installed at these stores detects the blacklisted person visiting their stores. At these stores, stickers are placed within the stores to inform customers that « face recognition security cameras are installed ». But customers are not informed that the stores are sharing the facial data.

Under Japanese law, facial images that are filmed by security cameras are considered personal information. The law allows such images to be filmed when it is used for crime prevention.

But sharing the facial data could be a violation of a law that bans providing personal information to a third party without the person's consent.

Lawyer Yoichiro Itakura said the data could be used in a way disadvantageous to customers as « stores can arbitrarily register specific shoppers as suspicious people, and they may then suffer unjust treatment at stores they have never visited before ».

An official of the Nagoya software development firm said: « The system has no problems. We just responded to the needs of the stores, which is their need to prevent shoplifting. »

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source :

<http://www.scmp.com/news/asia/article/1466536/115-japanese-stores-sharing-customers-facial-data>

Par Yomiuri Shimbun

# Systeme d'appel d'urgence (eCall) obligatoire à partir d'octobre 2015



## Systeme d'appel d'urgence (eCall) obligatoire à partir d'octobre 2015

A partir d'octobre 2015, tous les nouveaux véhicules vendus dans l'Union européenne seront équipés d'un service permettant de composer un numéro d'urgence en cas d'accident grave: le système eCall. C'est ce que prévoient les nouvelles règles qui seront votées par la commission du marché intérieur le 11 février 2014.

« eCall »: c'est le nom de ce système qui devrait sauver de nombreuses vies. En cas d'accident, le système eCall compose automatiquement le 112, et ce dès que ses capteurs (situés par exemple sur les airbags) enregistrent un choc. Le numéro pourrait également être activé manuellement, grâce à un bouton spécial. Le système est censé transmettre ensuite le lieu et l'heure de l'accident au centre de secours le plus proche.

« Le système eCall pourrait sauver jusqu'à 2500 vies par an, ce qui est selon moi un argument décisif pour l'introduction de ce service public d'appel d'urgence dans toute l'Union européenne », a déclaré le rapporteur Olga Sehnalová, députée démocrate socialiste tchèque.

D'ici là, les Etats membres devront améliorer leur infrastructure de manière à ce que les eCalls aboutissent directement aux services d'urgence.

Aujourd'hui, seuls 0,7 % de tous les passagers dans l'Union européenne sont équipés de systèmes automatiques d'appels d'urgence. Le coût d'une installation de l'outil eCall est estimé à moins de 100 euros par véhicule.

**Voir aussi sur le même sujet « Installation obligatoire d'eCall dans les véhicules à partir de 2015 »**

<http://www.techno-science.net/?onglet=news&news=11767>

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : <http://www.techno-science.net/?onglet=news&news=12481>

---

# 2015 sous haute tension en matière de Cybercriminalité



2015 sous haute  
tension en  
matière de  
Cybercriminalité

**Les cybercriminels sont de plus en plus confiants : ils avaient auparavant tendance à attaquer les usagers de services bancaires, voyant en eux le maillon faible de la chaîne de sécurité, mais les experts de Kaspersky Lab anticipent désormais des cyber-attaques ciblées d'envergure sur les banques elles-mêmes. Et les fraudeurs ne s'arrêteront pas là!**

Ils devraient tenter le tout pour le tout en essayant de développer de nouveaux malwares capables de retirer du liquide directement depuis les distributeurs. Outre les cyber-crimes financiers, 2015 suscitera probablement encore plus d'inquiétudes quant à la confidentialité et à la sécurité des appareils Apple, et fera resurgir les peurs quant aux appareils connectés ; il s'agira d'empêcher les hackers d'utiliser des outils comme les imprimantes réseau pour pénétrer les réseaux d'entreprises.

#### **1. Quand les cybercriminels s'inspirent des APT**

Lors d'une étude récente, nous avons découvert une attaque dans laquelle l'ordinateur d'un comptable a été compromis et utilisé pour effectuer un transfert important avec une institution financière. Cela illustre une tendance intéressante : celle des attaques ciblées contre les banques elles-mêmes.

Nous assistons à une augmentation des incidents provoqués par des malwares dans lesquels les banques sont infiltrées en utilisant des méthodes utilisées dans les APT. Une fois que les pirates ont pénétré les réseaux de la banque, ils volent assez d'informations pour pouvoir voler de l'argent directement à la banque et ce, de plusieurs manières :

- En prenant le contrôle des distributeurs automatiques à distance afin d'obtenir du liquide
- En réalisant des transferts SWIFT depuis plusieurs comptes de clients
- En manipulant les systèmes bancaires en ligne pour réaliser des transferts en arrière-plan

De telles attaques annoncent l'émergence d'une nouvelle tendance qui s'inspire des attaques APT que l'on voit dans le monde cybercriminel.

#### **2. Les groupes se fragmentent, les attaques APT se diversifient**

La révélation de l'existence de ces groupes utilisant les APT a mené à l'exposition publique et la condamnation d'un groupe de pirates qui aurait mené des actions de cyber-espionnage contre des entreprises américaines.

Alors que les équipes de recherche continuent d'encourager la découverte de ces groupes ayant recours aux APT, nous nous attendons à des changements en 2015 : les groupes d'APT les plus importants et les plus connus se sépareront en plus petits groupes qui fonctionneront indépendamment les uns des autres. Les attaques deviendront plus répandues et davantage d'entreprises seront touchées car les petits groupes diversifieront leurs attaques. Cela signifie également que les entreprises les plus importantes qui ont déjà été compromises dans le passé par deux ou trois groupes d'APT importants (comme par exemple, 'Comment Crew' et 'Webky') seront la cible d'attaques plus diverses et provenant de plusieurs sources différentes.

#### **3. Un ancien code, de nouvelles vulnérabilités (dangereuses)**

De récentes accusations d'altération délibérée et de défaillances accidentelles dans des systèmes de chiffrement (« goto fail ») ainsi que des vulnérabilités critiques dans des logiciels connus (Shellshock, Heartbleed, OpenSSL) ont laissé la communauté dubitative face à ces logiciels non vérifiés. La réaction a donc été de lancer des analyses indépendantes de la clé de ces logiciels ou que des chercheurs en sécurité les dissèquent à la recherche de vulnérabilités critiques (une alternative à l'analyse non officielle). Cela signifie que 2015 sera une autre année remplie de nouvelles vulnérabilités dangereuses qui apparaîtront dans des anciens codes, exposant ainsi l'infrastructure Internet à des attaques.

#### **4. Augmentation des attaques contre les distributeurs automatiques et les points de vente**

Les attaques contre les distributeurs automatiques semblent avoir explosé cette année avec plusieurs incidents publics et la vive réaction des autorités à travers le monde pour faire face à cette crise. Une des conséquences de ces incidents est la prise de conscience que ces distributeurs automatiques sont très faciles à pirater et les cybercriminels l'ont bien remarqué. Comme la plupart de ces systèmes fonctionnent sous Windows XP et disposent d'une sécurité physique très faible, ils sont très vulnérables par défaut. Et comme les institutions financières disposent d'argent liquide, il est logique que les cybercriminels commencent par là.

En 2015, nous nous attendons à observer une évolution de ces attaques contre les distributeurs automatiques grâce à l'utilisation de techniques d'APT afin d'accéder au système d'information de ces machines. On verra ensuite les pirates compromettre les réseaux des banques et utiliser cet accès pour prendre le contrôle des distributeurs en temps réel.

#### **5. Attaques Mac : des botnets OS X**

Malgré les efforts d'Apple pour verrouiller le système d'exploitation Mac, nous continuons d'observer des logiciels malveillants envoyés via des torrents ainsi que des logiciels piratés. La popularité grandissante des appareils Mac OS X fait tourner les têtes dans le monde criminel et rend très intéressante la création de malwares pour cette plateforme. L'écosystème fermé par défaut empêche les malwares d'envahir la plate-forme mais certains utilisateurs choisissent de désactiver les mesures de sécurité Mac OS X [ ] surtout ceux qui utilisent des logiciels piratés. Cela signifie que ceux qui cherchent à pirater les systèmes OS X pour diverses raisons savent qu'ils ont juste à cacher leur malware dans un logiciel attirant (certainement en le faisant passer pour un générateur de clé) pour réussir à le diffuser. À cause des idées reçues sur la plateforme OS X, ces systèmes ont peu de chances d'avoir une solution antimalware qui détectera les infections une fois le malware installé : ce dernier passera donc inaperçu pendant très longtemps.

#### **6. Des attaques contre les systèmes de billetterie automatique**

Les incidents comme le piratage NFC contre les transports publics chiliens (<http://securelist.com/blog/virus-watch/67283/android-nfc-hack-allow-users-to-have-free-rides-in-public-transportation>) montre l'intérêt que les criminels ont pour les ressources publiques comme les systèmes de transports publics. Certains pirates ne chercheront même pas à obtenir de l'argent pour ce type d'attaques et seront simplement contents de voyager gratuitement et de partager leur technique avec d'autres. Bien que ces systèmes de billetterie soient vulnérables (la plupart d'entre eux fonctionnent sous Windows XP), dans de nombreuses villes, ils gèrent directement des transactions par carte bancaire. Nous nous attendons donc à voir des attaques plus violentes contre ces systèmes que cela soit pour détourner le système ou voler des données de carte bancaire.

#### **7. Des attaques contre les systèmes de paiement virtuel**

La logique veut que les cybercriminels cherchent à gagner de l'argent grâce à leurs attaques de la manière la plus efficace et la plus simple possible. Quoi de mieux que les systèmes de paiement virtuel qui n'en sont encore qu'à leurs débuts ? Nous nous attendons donc à ce que les criminels se jettent sur toutes les opportunités qu'ils trouveront pour exploiter ces systèmes. Qu'il s'agisse d'ingénierie sociale, d'attaques ciblant les appareils des utilisateurs (dans la plupart des cas, les téléphones mobiles), ou de pirater directement des banques, les cybercriminels choisiront les attaques qui pourront leur rapporter de l'argent rapidement et les systèmes de paiement virtuel finiront par en faire les frais.

Ces craintes peuvent également s'appliquer à Apple Pay qui utilise la NFC (Near Field Communications) pour gérer les transactions sans fil des utilisateurs.

#### **8. Apple Pay**

De précédentes attaques se sont concentrées sur les systèmes de paiement NFC mais, grâce à son adoption limitée, ces attaques n'ont pas rapporté beaucoup. Apple Pay va certainement changer cela. L'enthousiasme pour ce nouveau système de paiement va faire exploser l'adoption de ce système et cela attirera bien évidemment les cybercriminels qui chercheront à intercepter ces transactions. Le design d'Apple se concentre principalement sur la sécurité (avec par exemple, la virtualisation des données de transaction) mais nous sommes très curieux de voir comment les pirates exploiteront les fonctionnalités de ce système.

#### **9. Compromettre l'Internet des objets**

Les attaques contre l'Internet des objets (ou objets connectés) se sont limitées aux prototypes et aux avertissements (parfois exagérés) annonçant que les smart TV et les réfrigérateurs seront ciblés par les pirates pour créer des Botnets ou lancer des attaques malveillantes.

Alors que de plus en plus d'appareils connectés sont disponibles, nous nous attendons à observer un débat plus important sur la sécurité et la confidentialité, surtout parmi les entreprises de ce secteur. En 2015, on verra certainement des attaques contre des imprimantes connectées en réseau et autres appareils connectés qui aideront les pirates expérimentés à s'infiltrer dans les réseaux corporatifs. Nous nous attendons à ce que les appareils de l'Internet des objets fassent partie de l'arsenal des groupes utilisant les APT, surtout si l'on considère que la connectivité est désormais introduite aux procédés industriels ainsi qu'aux procédés de fabrication.

Après cette lecture, quel est votre avis ?  
Cliquez et laissez-nous un commentaire...

Source : <http://www.economiatin.fr/news-2015-attaque-hacker-piratage-criminel-brulez>  
Par Nicolas Brulez

---

# Quand la technologie nous fait rêver : Fujitsu invente l'écran tactile sans écran

x	Quand la technologie nous fait rêver : Fujitsu invente l'écran tactile sans écran
---	---

**Aucun réel rapport avec la cybercriminalité et la protection des données personnelles, mais je ne peux rester insensible, lorsque la technologie m'impressionne. C'est une forme de morceau choisi de la technologie que j'avais envie de partager, avec vous : un écran tactile... sans écran, le papier tactile !**

*Fujitsu Laboratories has developed a next generation user interface which can accurately detect the users finger and what it is touching, creating an interactive touchscreen-like system, using objects in the real world.*

« We think paper and many other objects could be manipulated by touching them, as with a touchscreen. This system doesn't use any special hardware; it consists of just a device like an ordinary webcam, plus a commercial projector. Its capabilities are achieved by image processing technology. »

Using this technology, information can be imported from a document as data, by selecting the necessary parts with your finger.

This technology measures the shape of real-world objects, and automatically adjusts the coordinate systems for the camera, projector, and real world. In this way, it can coordinate the display with touching, not only for flat surfaces like tables and paper, but also for the curved surfaces of objects such as books.

« Until now, gesturing has often been used to operate PCs and other devices. But with this interface, we're not operating a PC, but touching actual objects directly, and combining them with ICT equipment. »

« The system is designed not to react when you make ordinary motions on a table. It can be operated when you point with one finger. What this means is, the system serves as an interface combining analog operations and digital devices. »

To detect touch accurately, the system needs to detect fingertip height accurately. In particular, with the low-resolution camera used here (320 x 180), if fingertip detection is off by a single pixel, the height changes by 1 cm. So, the system requires technology for recognizing fingertips with high precision.

« Using a low-res webcam gives a fuzzy picture, but the system calculates 3D positions with high precision, by compensating through image processing. »

This system also includes technology for controlling color and brightness, in line with the ambient light, and correcting for individual differences in hand color. In this way, it can identify fingertips consistently, with little influence from the environment or individual differences.

Also, in situations that don't use touch, the system can be operated by gesturing. In this demo, when you move your fist, you can manipulate the viewpoint for 3D CAD data. So, there could be applications for this touch system by combining it with current gesture systems.

« For example, we think this system could be used to show detailed information at a travel agent's counter, or when you need to fill in forms at City Hall. »

« We aim to develop a commercial version of this system by fiscal 2014. It's still at the demonstration level, so it's not been used in actual settings. Next, we'd like to get people to use it for actual tasks, see what issues arise, and evaluate usability. We want to reflect such feedback in this system. »

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : <http://mashable.com/2013/04/16/fujitsu-paper-touchscreen/>  
<http://www.diginfo.tv/v/13-0025-r-en.php>