

# Un oeil sur vous, citoyens sous surveillance – Documentaire 2015 | Denis JACOPINI

Un oeil sur vous, citoyens sous  
surveillance – Documentaire  
2015 2h24

**Des milliards de citoyens connectés livrent en permanence – et sans toujours s'en rendre compte – des informations sur leur vie quotidienne à des sociétés privées qui les stockent dans de gigantesques serveurs. Ces informations sont rendues accessibles aux États et vendues aux entreprises. Dans ce monde sous étroite surveillance, jusqu'où irons-nous en sacrifiant nos vies intimes et nos droits à la liberté individuelle ?**

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la #cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

Expert Informatique assermenté et formateur spécialisé en #sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

---

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

---

**Quoi et comment supprimer vos données si vous rendez votre ordinateur professionnel à votre employeur ?**



Quoi et comment  
supprimer vos  
données si vous  
rendez votre  
ordinateur  
professionnel à  
votre employeur ?



stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important) ?



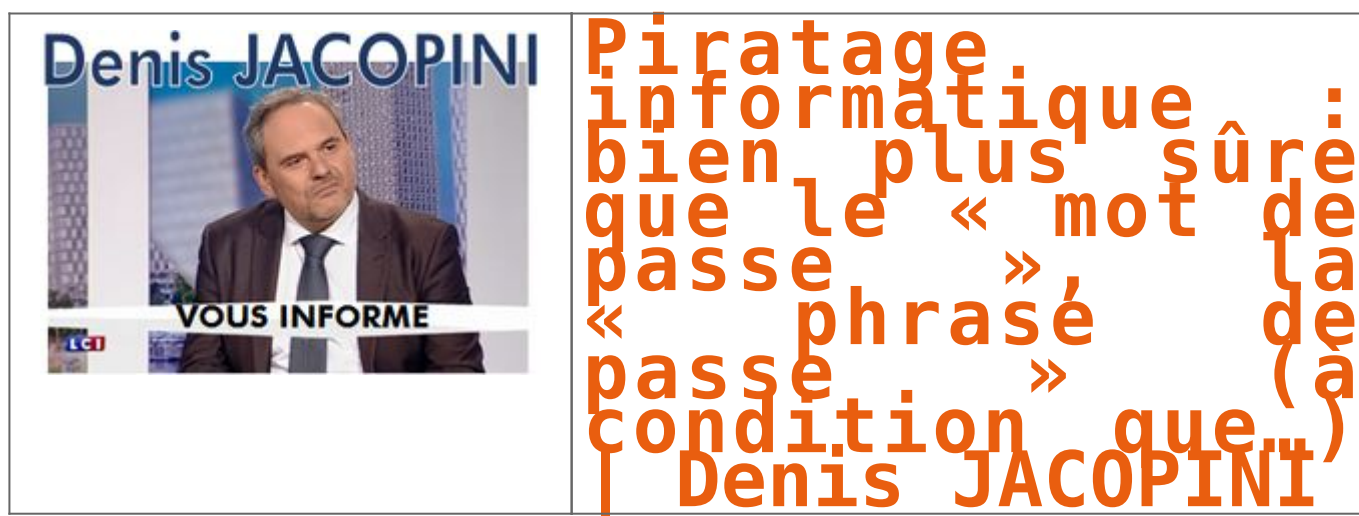
Étape par  
étape :  
comment bien  
effacer et  
conserver vos  
données  
informatiques  
stockées sur  
votre  
ordinateur  
professionnel  
si vous  
changez de  
travail à la  
rentrée (et  
pourquoi  
c'est très  
important) ?



Original de l'article mis en page : Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important) | Atlantico.fr

---

# Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que...) | Denis JACOPINI



Une « phrase de passe » est beaucoup plus difficile à pirater qu'un « mot de passe ». Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes et mettraient... plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

**Atlantico** : Selon de nombreuses études menées par des chercheurs de l'Université américaine Carnegie-Mellon, un long mot de passe facile à retenir tel que « *ilfaitbeaudanstoutelafrancesaufdanslebassinparisien* » serait plus difficile à pirater qu'un mot de passe relativement court mais composé de glyphes de toutes sortes, tel que « *p8)J#&=89pE* », très difficiles à mémoriser. Pouvez-vous nous expliquer pourquoi ?

**Denis Jacopini** : La plupart des mots de passe sont piratés par une technique qu'on appelle « la force brute ». En d'autres termes, les hackers vont utiliser toutes les combinaisons possibles des caractères qui composent le mot de passe.

Donc, logiquement, plus le mot de passe choisi va avoir de caractères (majuscule, minuscule, chiffre, symbole), plus il va être long à trouver. Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes via la technique de « la force brute », et mettraient... plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Un long mot de passe est donc plus difficile à pirater qu'un mot de passe court, à une condition cependant : que **la phrase choisie comme mot de passe ne soit pas une phrase connue de tous**, qui sort dès qu'on en tape les premiers mots dans la barre de recherche de Google. Les pirates du Net ont en effet des bases de données où ils compilent toutes les phrases, expressions ou mots de passe les plus couramment utilisés, et essaient de hacker les données personnelles en les composant tous les uns derrière les autres. Par exemple, mieux vaut avoir un mot de passe court et complexe plutôt qu'une « phrase de passe » comme « *Sur le pont d'Avignon, on y danse on y danse...* ».

Il faut également bien veiller à ce que cette « phrase de passe » ne corresponde pas trop à nos habitudes de vie, car les pirates du Web les étudient aussi pour arriver à leur fin. Par exemple, si vous avez un chien qui s'appelle « Titi » et que vous habitez dans le 93, il y a beaucoup de chance que votre ou vos mots de passe emploient ces termes, avec des associations basiques du type : « *jevaispromenermonchienTITIdansle93* ».

**De plus, selon la Federal Trade Commission, changer son mot de passe régulièrement comme il est habituellement recommandé aurait pour effet de faciliter le piratage. Pourquoi ?**

Changer fréquemment de mot de passe est en soi une très bonne recommandation, mais elle a un effet pervers : plus les internautes changent leurs mots de passe, plus ils doivent en inventer de nouveaux, ce qui finit par embrouiller leur mémoire. Dès lors, **plus les internautes changent fréquemment de mots de passe, plus ils les simplifient, par peur de les oublier, ce qui, comme expliqué plus haut, facilite grandement le piratage informatique.**

**Plus généralement, quels seraient vos conseils pour se prémunir le plus efficacement du piratage informatique ?**

Je conseille d'avoir une « phrase de passe » plutôt qu'un « mot de passe », qui ne soit pas connue de tous, et dont on peut aisément en changer la fin, pour ne pas avoir la même « phrase de passe » qui verrouille nos différents comptes.

Enfin et surtout, je conseille de ne pas se focaliser uniquement sur la conception du mot de passe ou de la « phrase de passe », parce que c'est très loin d'être suffisant pour se prémunir du piratage informatique. Ouvrir par erreur un mail contenant un malware peut donner accès à toutes vos données personnelles, sans avoir à pirater aucun mot de passe. Il faut donc rester vigilant sur les mails que l'on ouvre, réfléchir à qui on communique notre mot de passe professionnel si on travail sur un ordinateur partagé, bien verrouiller son ordinateur, etc...

Article original de Denis JACOPINI et Atlantico

---

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>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (Investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

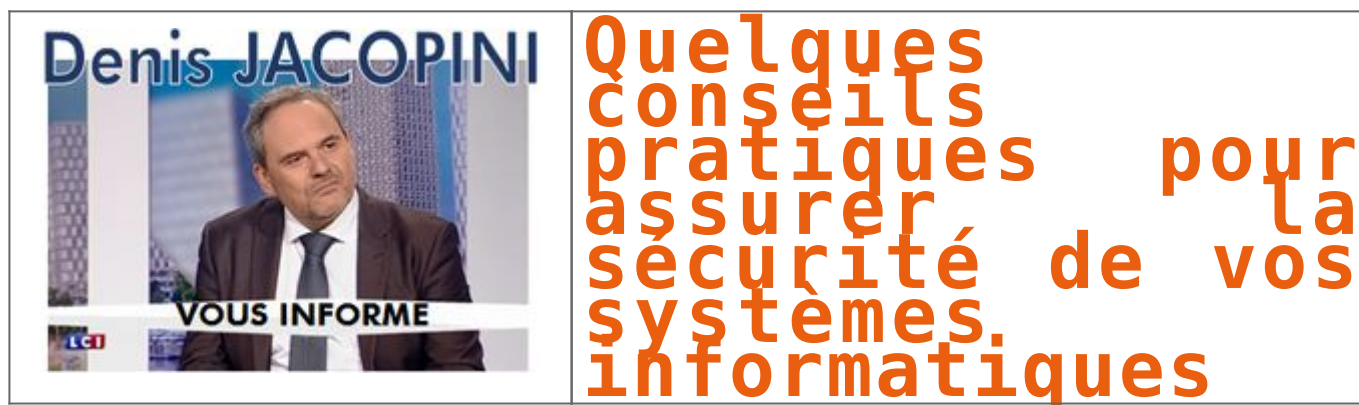
Réagissez à cet article



Original de l'article mis en page : Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que...) | Atlantico.fr

---

# Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques





Original de l'article mis en page : Conseils aux usagers | Gouvernement.fr

# Comment sécuriser Firefox efficacement en quelques clics de souris ?

 <p>Attention, danger !</p> <p>La modification de ces préférences avancées peut être dommageable pour la stabilité, la sécurité et les performances de cette application. Ne continuez que si vous savez ce que vous faites.</p> <p><input checked="" type="checkbox"/> Afficher cet avertissement la prochaine fois</p> <p><a href="#">Je ferai attention, promis !</a></p>	<p>Comment sécuriser Firefox efficacement en quelques clics de souris ?</p>
---	---

**Vous utilisez Firefox et vous souhaitez que cet excellent navigateur soit encore plus sécurisé lors de vos surfs sur Internet ? Voici quelques astuces qui supprimeront la géolocalisation, le profilage de Google ou encore que vos données offline disparaissent du regard d'espions locaux.**

C'est sur le blog des Télécoms que j'ai vu pointer l'information concernant le réglage de plusieurs paramètres de Firefox afin de rendre le navigateur de la fondation Mozilla encore plus sécurisé. L'idée de ce paramétrage, empêcher par exemple Google de vous suivre à la trace ou de bloquer la géolocalisation qui pourrait être particulièrement big brotherienne.

Commençons par du simple. Il suffit de taper dans la barre de navigation de votre Firefox la commande `about:config`. Une alerte s'affiche, pas d'inquiétude, mais lisez là quand même. recherchez ensuite la ligne `security.tls.version`. Les valeurs affichées doivent osciller entre 1 et 3. Ensuite, recherchez la ligne `geo.enabled` pour annuler la géolocalisation. Passez le « true » en « False ». Pour que les sites que vous visitiez ne connaissent pas la dernière page que vous avez pu visiter, cherchez la ligne `network.http.sendRefererHeader` et mettez la valeur 1. Elle est naturellement placée à 2. Passez à False la ligne `browser.safebrowsing.malware.enabled`.

Ici, il ne s'agit pas d'autoriser les malwares dans Firefox, mais d'empêcher Google de vous tracer en bloquant les requêtes vers les serveurs de Google. Pour que Google cesse de vous profiler, cherchez la ligne `browser.safebrowsing.provider.google.lists` et effacez la valeur proposée.

Pour finir, vos données peuvent être encore accessibles en « offline », en mode hors connexion. Cherchez les lignes `offline-apps.allow_by_default` et `offline-apps.quota.warn`. La première valeur est à passer en False, la seconde valeur en 0.

Il ne vous reste plus qu'à tester votre navigateur via le site de la CNIL ou celui de l'Electronic Frontier Foundation.

Article original de Damien Bancal



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet..) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Original de l'article mis en page : Sécuriser Firefox efficacement en quelques clics de souris – Data Security BreachData Security Breach

**Victime d'une arnaque sur Internet ? Faites-nous part de votre témoignage**

 <p><b>ARNAQUE</b></p>	<p>Victime d'une arnaque sur Internet ? Faites-nous part de votre témoignage</p>
---	--

**Vous êtes victime d'une arnaque ou d'un piratage sur Internet ? Votre témoignage nous permettra peut-être de vous aider.**

Devant une explosion de cas d'arnaques et de piratages par Internet et des pouvoirs publics débordés par ce phénomène, nous avons souhaité apporter notre pierre à l'édifice.

Vous souhaitez nous faire part de votre témoignage, contactez-nous.

Vous devez nous communiquer les informations suivantes (tout message incomplet et correctement rédigé ne sera pas traité) :

- une présentation de vous (qui vous êtes, ce que vous faites dans la vie et quel type d'utilisateur informatique vous êtes) ;
- un déroulé chronologique et précis des faits (qui vous a contacté, comment et quand et les différents échanges qui se sont succédé, sans oublier l'ensemble des détails même s'ils vous semblent inutiles, date heure, prénom nom du ou des interlocuteurs, numéro, adresse e-mail, éventuellement numéros de téléphone ;
- Ce que vous attendez comme aide (je souhaite que vous m'aidiez en faisant la chose suivante : ....)
  - Vos nom, prénom et coordonnées (ces informations resteront strictement confidentielles).

Contactez moi

Conservez précieusement toutes traces d'échanges avec l'auteur des actes malveillants. Ils me seront peut-être utiles.



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

La sensibilisation des utilisateurs est la principale clé pour se protéger des pirates informatiques. Il n'est pas trop tard !



La sensibilisation des utilisateurs est la principale clé pour se protéger des pirates informatiques. Il n'est pas trop tard !

### La sensibilisation des utilisateurs est la clé pour se protéger des pirates informatiques

L'avis de Denis JACOPINI, Expert informatique assermenté spécialisé en cybercriminalité (arnaques, virus, phishing...) en Direct sur LCI le 23 mai 2016 dans l'émission « Ca nous Concerne » de Valérie Expert.

En mai 2016, Denis JACOPINI nous sensibilisait encore et déjà aux **cyber risques**.

Nos formations / nos sensibilisations  
Toutes nos vidéos

LE NET EXPERT ET DENIS JACOPINI FONT DÉSORMAIS PARTIE  
DES PRESTATAIRES DE CONFIANCE DE LA PLATEFORME



#### LE NET EXPERT

- ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX → MISE EN CONFORMITÉ)
  - ANALYSE DE VOTRE ACTIVITÉ
  - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
    - IDENTIFICATION DES RISQUES
    - ANALYSE DE RISQUE (PIA / DPIA)
  - MISE EN CONFORMITÉ RGPD de vos traitements
  - SUIVI de l'évolution de vos traitements
    - FORMATIONS / SENSIBILISATION :
      - CYBERCRIMINALITÉ
    - PROTECTION DES DONNÉES PERSONNELLES
      - AU RGPD
      - À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
  - ORDINATEURS (Photos / E-mails / Fichiers)
  - TÉLÉPHONES (récupération de Photos / SMS)
  - SYSTÈMES NUMÉRIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
  - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
    - SÉCURITÉ INFORMATIQUE
    - SYSTÈMES DE VOTES ÉLECTRONIQUES

#### Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- **Mise en conformité RGPD** ;
- Accompagnement à la mise en place de DPO ;
- **Formations** (et sensibilisations) à la **Cybercriminalité** (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et Judiciaires ;
- **Recherche de preuves** : téléphones, disques durs, e-mails, contenus, détournements de clientèle... ;
- **Expertises de systèmes de vote électronique** ;



Contactez-nous

Réagissez à cet article

# Comment se préparer aux incidents de sécurité ?



Comment se préparer aux incidents de sécurité ?





**Les entreprises doivent être prêtes à agir face à des incidents de sécurité et à des attaques. Et cela passe notamment par sept points précis (par Peter Sullivan).**

Un plan de préparation à la cybersécurité présente et détaille les objectifs fondamentaux que l'organisation doit atteindre pour se considérer comme prête à faire face à des incidents de sécurité informatique. La liste de contrôles qui va suivre n'est pas exhaustive, mais elle souligne des objectifs qui constituent un minimum requis pour donner un niveau raisonnable de sensibilisation à la cybersécurité et se concentrer sur la protection des actifs informationnels essentiels.

Ici, la préparation à la cybersécurité est définie comme l'état permettant de détecter et de réagir efficacement aux brèches et aux intrusions informatiques, aux attaques de logiciels malveillants, aux attaques par hameçonnage, au vol de données et aux atteintes à la propriété intellectuelle – tant à l'extérieur qu'à l'intérieur du réseau.

Un élément essentiel de cette définition est de « pouvoir détecter ». La détection est un domaine où une amélioration significative peut être atteinte en abaissant le délai de détection, couramment observé entre 9 et 18 mois. Une capacité de détection plus rapide permet de limiter les dommages causés par une intrusion et de réduire le coût de récupération de cette intrusion. Être capable de comprendre les activités régulières du réseau et de détecter ce qui diverge de la norme est un élément important de la préparation à la cybersécurité. Voici une sept objectifs que les entreprises devraient considérer.

## Les objectifs à atteindre

1. Plan de cybersécurité
2. Gestion du risque
3. Gestion de l'identité
  - Contrôle d'accès
  - Authentification
  - Autorisation
  - Responsabilité
4. Surveillance de réseau
5. Architecture de sécurité
6. Contrôle des actifs, des configurations et des changements
7. Cartographie de la gestion des incidents

...[lire la suite]

---

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Se préparer aux incidents de sécurité*

---

# Les bons réflexes contre les attaques informatiques | Denis JACOPINI

x	Les bons réflexes contre les attaques informatiques
---	--

350 milliards d'euros par an : selon le McAfee Report on the Global Cost of Cybercrime publié en 2014, tel est le coût estimé des attaques informatiques à l'échelle mondiale. Depuis le début de l'année, les attaques se sont multipliées, notamment suite aux attentats de Charlie Hebdo, mettant plus que jamais en péril la sécurité des données des entreprises et des institutions. Un rapport publié le 16 février dernier par Kaspersky Lab a quant à lui révélé l'attaque d'une certaine de banques depuis 2013 par un gang organisé.

Afin d'appréhender au mieux ces offensives, il est important d'en comprendre les tenants et les aboutissants et d'avoir à l'esprit les réflexes qui permettent de s'en prémunir.

#### Des attaques aux motivations multiples

De plus en plus de sites internet sont victimes d'attaques dites de « défiguration » perpétrées par des hacktivistes revendiquant des convictions religieuses, politiques ou encore contestataires. On trouve également certains attaquants qui agissent uniquement pour l'amusement, mais ces scénarios se font de plus en plus rares. En général, seule la page d'accueil du site est modifiée pour signifier leur passage et évoquer leurs revendications.

On trouve également d'autres attaques qui, elles, sont plus furtives (ou en tout cas tentent de l'être) et consistent à voler des informations à des fins de rançonnement par exemple. Les vols de données bancaires (carte de crédit, numéros de comptes) permettent quant à eux du détournement d'argent, l'achat de services ou encore de matériels en ligne. Ces criminels, bien organisés, offrent des services de tout type à d'autres criminels : du kit d'infection, à l'envoi de spam massif, en passant par des serveurs de contrôle (C&C) pilotant des milliers de machines « zombies » permettant des attaques DDoS (Déni de service distribués). Tous n'ont pas le même niveau technique, certains ne sont d'ailleurs que des « presse-bouton », alors que d'autres ont la capacité de créer des virus, ou des programmes exploitant des failles de sécurité.

Mais comment s'y prennent-ils ? Ces malfaiteurs utilisent une faille de sécurité dans un programme qui peut provenir d'une erreur de conception (un protocole mal sécurisé par exemple), de programmation ou d'implémentation (failles connues comme shellshock, heartbleed ou ghost), de configuration (oubli du mot de passe par défaut après une installation) ou encore d'une erreur d'utilisation par une personne utilisant un mot de passe trop faible par exemple. L'humain est donc au centre de cette problématique.

Le plus souvent ces attaques débouchent sur du détournement d'argent ou la diffusion de données sur internet. Les conséquences financières pour les entreprises peuvent être considérables, sans compter l'impact que cela peut avoir sur l'image de l'entreprise victime d'un piratage. Dès lors, quels réflexes adopter face à ces diverses attaques et failles ?

Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.

Contactez-nous

#### Adopter les bonnes pratiques pour limiter les risques

Les attaques ne cessent de croître dans la mesure où l'enjeu financier pour les criminels est très important. Lorsque l'on sait que l'attaque par déni de service est accessible pour seulement 30 à 70 dollars la journée et qu'un spam ne revient qu'à 10 dollars par tranche d'un million d'e-mails\*, ce type de pratique n'est pas prêt de cesser. A ce premier enjeu s'ajoute le manque de vigilance dont font preuve les internautes. Le risque de s'infecter est en effet omniprésent : il suffit de cliquer sur un lien drainant un logiciel malveillant ou encore de partager un contenu infecté.

Quand bien même le risque zéro n'existe pas, la grande majorité de ces attaques pourrait être bloquée, dès lors que l'on adopte les bonnes pratiques pour se protéger et protéger autrui. Le maître mot est l'anticipation et la capacité à réagir rapidement en cas d'intrusion, la mise en œuvre d'un pare-feu ou d'un anti-virus pour se protéger n'étant pas suffisante. Le processus organisationnel de sécurisation est en effet plus important que les outils de protection eux-mêmes (on a en général un rapport de 80-20).

Pour ce faire, l'un des points majeurs est la gestion des mises à jour. Lorsqu'une faille tombe, celle-ci peut-être déjà exploitée plus ou moins massivement. S'en suit la douloureuse phase consistant à tester si le programme régresse ou non dans son fonctionnement avant une mise en production. Durant toute cette période, le programme est encore exposé à une potentielle exploitation de la faille. Cela sous-entend qu'il faut d'une part valider aussi vite que possible, et d'autre part essayer de se protéger temporairement avec des outils de type Firewall ou IPS. Il est aussi bon de rappeler que ces outils de protection sont aussi fallibles que les autres et qu'ils peuvent être contournés.

Dans le cas où l'attaque a déjà eu lieu, sur un site web par exemple, la première chose à faire est de bloquer le site. Cette phase est primordiale dans la mesure où un site piraté peut renvoyer des logiciels malveillants aux internautes le consultant. La deuxième étape est de sauvegarder tous les journaux, les données et programmes du site ainsi que la base de données, avant de procéder à une analyse du système pour connaître l'origine de l'attaque. Cette analyse est primordiale pour une remise en production du site. Elle permet de connaître par quel moyen les attaquants sont entrés dans le système et ce qu'il faut mettre à jour. Le mieux est de revenir sur une version de sauvegarde dont on est sûr qu'elle n'a pas été affectée par la compromission et de la mettre à jour. Parallèlement, il est également vivement conseillé de porter plainte afin que ces attaques soient référencées par les autorités et que des mesures soient prises.

S'il est crucial de prendre en compte la problématique de sécurité lors de la création d'un projet informatique, il est tout aussi indispensable d'en assurer la maintenance afin d'anticiper les attaques et de pouvoir les gérer efficacement, et ainsi minimiser leur impact sur l'activité de l'entreprise.

Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire.

Source : <http://www.journaldunet.com/solutions/expert/60882/attaques-informatiques-decryptage-du-phenomene-et-reflexes-a-adopter.shtml>  
Par Sébastien Delcroix – NFrance