# Sensibilisation aux arnaques aux petites annonces


## Sensibilisation aux arnaques aux petites annonces

---

**Vous feriez confiance à cet homme ? Sur Internet aussi, soyez vigilants: il arrive que des acheteurs ou vendeurs malhonnêtes essaient de vous arnaquer. Découvrez les bons réflexes sécurité avec PayPal. Acheter et vendre en ligne est simple et sécurisé avec PayPal, 7 millions de Français nous utilisent déjà.**

## Campagne Paypal France 2016

---

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

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

Le Net Expert
INFORMATIQUE
*Consultant en Cybercriminalité et en Protection des Données Personnelles*

Contactez-nous

Réagissez à cet article

# La France adopte son arsenal anti-hackers

| | |
|---|---|
|  | La France adopte son arsenal anti-hackers |

**La loi de programmation militaire a placé le secteur financier en première ligne des 12 opérateurs d'importance vitale, soumis à de nouvelles règles de sécurité.**

C'est un test d'envergure pour les banques françaises. L'Etat a placé le secteur financier en première ligne des douze secteurs d'importance vitale qui devront adopter les nouvelles règles en matière de cybersécurité, arrêtées par la loi de programmation militaire de 2013.
Ce choix n'est pas dû à une recrudescence des cyber-risque dans le secteur, assure la puissance publique – en l'occurrence, c'est Bercy qui a fait l'objet de l'attaque la plus grave ayant jamais visé une administration en France en 2011. *« Le niveau de sécurité du secteur financier est jugé satisfaisant,* indique Yves Jussot, coordinateur sectoriel à l'Agence nationale de la sécurité des systèmes d'information (Anssi). *Cependant la menace évolue vite et de façon continue, en particulier avec le développement du numérique. »*
Considérées comme *« pionnières »* dans l'identification des menaces informatiques et de lutte contre les cyberfraudes, les banques fixeront la barre des nouvelles exigences en matière de protection, qui s'appliqueront aux autres secteurs vitaux comme l'énergie, aux transports, en passant par la santé. Définies par un arrêté d'ici au 1er juillet, celles-ci promettent d'être élevées. Des règles renforcées en matière d'administration des systèmes sont par exemple définies pour cantonner davantage les flux de données.
Surtout, l'Etat voit son pouvoir renforcé en matière de contrôle. L'Anssi, rattachée au secrétaire général de la Défense et de la sécurité nationale, pourra mener des audits réguliers, et des amendes pourront être délivrées pour infraction à la sécurité informatique ou non-application de la réglementation. Les incidents qui pouvaient jusqu'à présent ne pas être déclarés devront être notifiés et, en cas d'attaque majeure, l'Anssi pourra prendre la main sur les systèmes. L'Etat a pris soin de travailler de concert avec les banques, au travers du Forum des compétences, qui regroupe les experts informatiques des banques et des assurances. Restera la question des moyens. *« La course à la transformation digitale entre banques impose d'aller vite et d'y allouer des moyens. La mise à niveau des systèmes informatiques peut ne pas suivre et ne pas être prioritaire »*, note un expert en cybersécurité…[Suite de l'article original de Anne RIF et Véronique CHOCRON]

---



Réagissez à cet article

Source : *La France adopte son arsenal anti-hackers, Banque – Assurances*

---

# Blogueurs, attention aux

# promesses des Publicités …


## Blogueurs, attention aux promesses des Publicités …

**Publicité malveillante – Elles se nomment Elena, Yoana, Elise… elles sont toutes éditrices indépendantes et recherchent des espaces publicitaires sur votre blog. Attention, piège à la Publicité malveillante pour casinos.**

Des courriers et autres sollicitations commerciales sont légions dans le monde des blogueurs. Achats d'espaces publicitaires, d'articles ou de liens sponsorisés sont des demandes constantes dès qu'un site fonctionne et attire les internautes. Je vais cependant vous mettre en garde contre des promesses venues du ciel 2.0. « ***Bonjour, je me présente, je m'appelle Yoana et je suis une éditrice indépendante. Je suis intéressée par l'achat d'un espace publicitaire sur votre site http://www.zataz.com . Je souhaite acheter la publication pour un de nos articles, qui contiendra un ou plusieurs liens internes.***«
L'espace entre l'url est important à prendre en compte, je vais vous expliquer pourquoi. Les espaces situés entre le début et la fin de l'adresse Internet sont générés par un logiciel qui automatise les courriels. Bilan, Elena, Yoana, Elise… ne savent pas qui vous êtes. Elles (ou ils), il s'agit aussi très certainement de la même personne officiant d'Italie et d'Israel, espèrent une réponse de votre part. Ne mordez pas à son hameçon. « ***Je peux payer via Paypal sous 24/48h*** » stipulent les interlocutrices.

***Publicité malveillante***
*Mais que proposent donc ces « dames » ? Tout simplement… des articles et des liens renvoyant sur de faux blogs dédiés aux Casinos. L'idée est simple, plus il y aura de liens vers ces faux blogs, plus ils seront référencés. Plus ils seront référencés, plus les internautes auront envie de cliquer sur les autres adresses Internet proposées par ces faux blogs. Des urls qui dirigent tous vers des casinos illicites, interdits en France.*
*Elena, Yoana, Elise… ne vendent pas les liens directs vers ces casinos, mais pièges les blogueurs qui seraient tentés. Bref, ne sombrez pas aux sons de ses Calliopes car le prochain son que vous pourriez entendre risque d'être celui d'une convocation par le service central des courses et jeux de la Direction Centrale de la Police Judiciaire.*

***Fausse publicité mais vrai piège***
*Les sommes varient pour cette publicité malveillante. Selon son emplacement de l'article, sa durée de mise en ligne. J'ai pu constater des propositions pécuniaires, qui m'étaient faites, pouvant aller de 200 à 1.500€. Autant dire que pour un blogueur, la manne financière est loin d'être négligeable. D'autant plus que Elena, Yoana, Elise… fournissent le texte, les photos, les liens. Malines, quelques jours après la diffusion de l'article en question, elles demandent une modification dans les urls, les ancres dédiées à certains mots du texte. Une manipulation permettant un référencement plus « musclé » dans les moteurs de recherche. « **C'était de l'argent facile**, me confiait il y a quelques temps Clément [prénom modifié], un blogueur. **Mon post était en ligne à 16h. J'ai reçu mon paiement à 20h. J'ai modifié l'article et les liens le lendemain. Une semaine plus tard je recevais un avertissement de l'ARJEL... et une convocation devant les policiers.***

***L'ARJEL veille***
*Ce qu'oublient de dire les mystérieuses sirènes, les sites qu'elles souhaitent mettre en avant dans la publicité malveillante commercialisée ne sont pas reconnues par l'ARJEL, l´Autorité de Régulation des Jeux en Ligne veille. En France, depuis le 12 mai 2010, l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne ne permet plus aux blogueurs d'afficher n'importe quel site dédié aux casinos. Une loi qui s'applique à toute personne proposant, en France, une offre de jeux d'argent et de hasard en ligne. Bref, diffuser un article, des liens, vers des casinos et autres portails dédiés aux jeux de hasard non titulaires de l'agrément ARJEL, peut entraîner de sérieux ennuis aux blogueurs ne respectant pas la loi : « **Quiconque fait de la publicité, par quelque moyen que ce soit, en faveur d'un site de paris ou de jeux d'argent et de hasard non autorisé en vertu d'un droit exclusif ou de l'agrément prévu à l'article 21 est puni d'une amende de 100 000 €. Le tribunal peut porter le montant de l'amende au quadruple du montant des dépenses publicitaires consacrées à l'activité illégale. Ces peines sont également encourues par quiconque a, par quelque moyen que ce soit, diffusé au public, aux fins de promouvoir des sites de jeux en ligne ne disposant pas de l'agrément prévu à l'article 21, les cotes et rapports proposés par ces sites non autorisés.**«
Elena, Yoana, Elise… ne risquent rien, elles sont à l'étranger (Italie, Israël…). En France, 3 ans de prison et 90.000€ d'amende pour « **Quiconque aura offert ou proposé au public une offre en ligne de paris ou de jeux d'argent et de hasard sans être titulaire de l'agrément mentionné à l'article 21 ou d'un droit exclusif**« . Des peines portées à sept ans d'emprisonnement et à 200 000 € d'amende lorsque l'infraction est commise en bande organisée… [Lire la suite]*

*Merci à Damien BANCAL l'auteur de cet article pour toutes ces précieuses informations.*

---



*Réagissez à cet article*

Source : *ZATAZ Publicité malveillante : Piége à blogueur – ZATAZ*

---

# Augmentation de 30% des demande de rançon informatique en 3 mois

| | |
|---|---|
|  | **Augmentation de 30% des demande de rançon informatique en 3 mois** |

---

**Le #ransomware a dépassé les attaques de type APT (menaces persistantes avancées) pour devenir le principal sujet d'actualité du trimestre. 2900 nouvelles variantes de malwares au cours de ces 92 jours.**

Selon le rapport de Kaspersky Lab sur les malwares au premier trimestre, les experts de la société ont détecté 2900 nouvelles variantes de malwares au cours de cette période, soit une augmentation de 14 % par rapport au trimestre précédent. 15 000 variantes de ransomware sont ainsi dorénavant recensés.

**Un nombre qui va sans cesse croissant.**
Pourquoi ? Comme j'ai pu vous en parler, plusieurs kits dédiés aux ransomwares sont commercialisés dans le blackmarket. Autant dire qu'il devient malheureusement très simple de fabriquer son arme de maître chanteur 2.0.
Au premier trimestre 2016, les solutions de sécurité de l'éditeur d'antivirus ont empêché 372 602 attaques de ransomware contre leurs utilisateurs, dont 17 % ciblant les entreprises. Le nombre d'utilisateurs attaqués a augmenté de 30 % par rapport au 4ème trimestre 2015. Un chiffre à prendre avec des pincettes, les ransomwares restant très difficiles à détecter dans leurs premiéres apparitions.

**Locky , l'un des ransomwares les plus médiatisés et répandus au 1er trimestre**
Le ransomware Locky est apparu, par exemple, dans 114 pays. Celui-ci était toujours actif début mai. Un autre ransomware nommé Petya est intéressant du point de vue technique en raison de sa capacité, non seulement à crypter les données stockées sur un ordinateur, mais aussi à écraser le secteur d'amorce (MBR) du disque dur, ce qui empêche le démarrage du système d'exploitation sur les machines infectées.
Les trois familles de ransomware les plus détectées au 1er trimestre ont été Teslacrypt (58,4 %), CTB-Locker (23,5 %) et Cryptowall (3,4 %). Toutes les trois se propagent principalement par des spams comportant des pièces jointes malveillantes ou des liens vers des pages web infectées. « Une fois le ransomware infiltré dans le système de l'utilisateur, il est pratiquement impossible de s'en débarrasser sans perdre des données personnelles. » confirme Aleks Gostev, expert de sécurité en chef au sein de l'équipe GReAT (Global Research & Analysis Team) de KL.

**Une autre raison explique la croissance des attaques de ransomware** : les utilisateurs ne s'estiment pas en mesure de combattre cette menace. Les entreprises et les particuliers n'ont pas conscience des contre-mesures technologiques pouvant les aider à prévenir une infection et le verrouillage des fichiers ou des systèmes, et négligent les règles de sécurité informatique de base, une situation dont profitent les cybercriminels entre autres. Bref, trop d'entreprise se contente d'un ou deux logiciels de sécurité, se pensant sécurisées et non concernées. L'éducation du personnel devrait pourtant être la priorité des priorités… [Lire la suite]

Article 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.

Le Net Expert INFORMATIQUE
Consultant en Cybersécurité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Ransomware: +30% d'attaques en 3 mois – Data Security BreachData Security Breach*

---

# Un gros botnet détourne des requêtes de recherche


Un gros botnet détourne des requêtes de recherche

---

**Depuis septembre 2014, un botnet a pu compter près d'un million de zombies pour faire gonfler des revenus publicitaires de cybercriminels.**


Actif depuis mi-septembre 2014, un botnet est parvenu à prendre le contrôle de près d'un million d'ordinateurs dans le monde. L'agent infectieux est un malware intégré dans un fichier d'installation modifié de type MSI pour Windows.
Botnet-Redirector.Paco-carte-BitdefenderCes fichiers corrompus sont associés à des programmes tels que WinRAR, YouTube Downloader, Connectify, Start8 et KMSPico. Après installation sur la machine prise pour cible, le nuisible dénommé Redirector.Paco s'appuie sur un fichier PAC (Proxy auto-config) pour rediriger des requêtes de recherches sur Google, Bing ou Yahoo.
Au gré de quelques modifications dans la base de registre, le trafic sera redirigé vers des publicités contextuelles permettant de générer des revenus ici frauduleux grâce au programme AdSense pour les recherches de Google.
Les opérateurs du botnet détournent les recherches vers un autre moteur de recherche personnalisé spécifiquement conçu qui affiche ses propres résultats, et détournent par la même occasion des revenus publicitaires… [Lire la suite]
Article de Jérôme GARAY

---

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

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

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Un gros botnet détourne des requêtes de recherche*

---

# Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue

Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue

---

**Les chercheurs d'ESET découvrent un malware qui a échappé à la surveillance des chercheurs d'antivirus depuis au moins 2008. Ce malware, nommé Win32/Prikormka et détecté par ESET comme malware utilisé pour mener des activités de cyber-espionnage, cible principalement les séparatistes anti-gouvernementaux des républiques autoproclamées de Donetsk et Luhansk.**

« Avec la crise ukrainienne de l'EST du pays, ce dernier a connu de nombreuses cyber-attaques ciblées ou de menaces persistantes avancées (APTs). Nous avons découvert par le passé plusieurs attaques utilisant des logiciels malveillants tels que BlackEnergy qui avait entraîné une panne d'électricité. Mais dans l'opération **Groundbait**, l'attaque utilise des logiciels malveillants qui n'avaient encore jamais été utilisés. », explique Robert Lipovský, ESET Senior Malware Researcher.
Le vecteur d'infection principalement utilisé pour diffuser les logiciels malveillants dans l'opération Groundbait est le spear-phishing. «Au cours de nos recherches, nous avons observé un grand nombre d'échantillons ayant chacun son numéro de campagne ID désigné, avec un nom de fichier attrayant pour susciter l'intérêt de la cible. », explique Anton Cherepanov, Malware Researcher chez ESET.
L'opération a été nommée **Groundbait** (appât) par les chercheurs d'ESET suite à l'une des campagnes des cybercriminels. Alors que la majorité des autres campagnes utilisent les thèmes liés à la situation géopolitique actuelle de l'Ukraine et la guerre de Donbass pour attirer les victimes dans l'ouverture de la pièce jointe, la campagne en question, elle, affiche une liste de prix d'appâts de pêche à la place.
« Pour l'heure, nous ne sommes pas en mesure d'expliquer le choix de ce document comme leurre », ajoute Lipovský.
Comme c'est souvent le cas dans le monde de la cybercriminalité et des APTs, il est difficile de trouver la source de cette attaque. Nos recherches à ce sujet ont montré que les cybercriminels viennent très probablement de l'intérieur de l'Ukraine. Quoi qu'il en soit et au vu des cibles choisies, il est probable que cette opération de cyber-surveillance soit nourrie par une motivation politique. « En dehors de cela, toute nouvelle tentative d'attribution serait à ce point spéculatif. **Il est important de noter que, outre les séparatistes, les cibles de cette campagne sont les responsables gouvernementaux ukrainiens, les politiciens et les journalistes.** La possibilité de l'existence de fausses bannières doit également être prise en compte. », conclut Robert Lipovský.

Vous trouverez davantage de détails au sujet de l'opération Groundbait ici.

Article de Benoit Grunemwald
Directeur Commercial & Marketing ESET France

---



Réagissez à cet article

Source : *Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue*

---

# Un hôpital paye la rançon mais n’obtient rien en échange.


## Un hôpital paye la rançon mais n’obtient rien en échange

---

**Certains groupes de pirates qui exploitent des ransomwares pour faire fortune sans effort n'ont ni morale ni parole, si l'on en croit la prise en otage de données d'un hôpital, qui a payé pour rien la rançon demandée.**

Les maître-chanteurs sont aussi parfois de véritables escrocs, et ça n'est jamais une bonne idée de céder à leurs exigences. Après la messagerie chiffrée Protonmail qui avait payé une rançon et avait malgré tout continué à subir des attaques DDOS massives, c'est un hôpital américain qui l'apprend à ses dépens.

Ainsi Network World rapporte que le Kansas Heart Hospital à Wichita a accepté de payer une rançon après que des pirates ont réussi à infecter son système informatique avec un ransomware, qui chiffre les données stockées avec une clé que seul le ravisseur connaît. Ce n'est pas le premier hôpital à être visé et à céder ainsi à un chantage informatisé, mais c'est la première fois que les pirates ne respectent pas leur part du marché. Pire, ils en demandent plus.

## PAYER ENCORE POUR DÉBLOQUER UN PEU PLUS

L'attaque avait eu lieu la semaine dernière, et avait rendu des fichiers de l'hôpital inaccessibles, sans possibilité de recourir à des archives. Pour les débloquer, il fallait payer de l'argent en utilisant un service anonymisé, sur Tor, avec un compte en bitcoins intraçable. Étant donnée l'importance des données, les administrateurs de l'établissement ont accepté de payer une somme indéterminée, relativement faible. Mais plutôt que de déchiffrer les données, les pirates n'en ont libéré qu'une petite partie, et exigé davantage d'argent pour déchiffrer le reste.

L'hôpital a alors refusé. « Ce n'était plus une manœuvre sage ou une stratégie », s'est justifiée la direction, qui a mis en place un plan B pour limiter les effets de l'attaque. Selon le Kansas Heart Hospital, aucun patient n'a eu à subir d'effets négatifs en raison de l'indisponibilité de certaines données… [Lire la suite]

---



Réagissez à cet article

Source : *Ransomware : un hôpital paye la rançon mais n'obtient rien en échange – Business – Numerama*

Auteur : Guillaume Champeau

# 11 millions volés dans une attaque simultanée de distributeurs automatiques


11 millions volés dans une attaque simultanée de distributeurs automatiques

**Au Japon, des pirates ont réussi à dérober 1,4 milliard de yens (11 millions d'euros) à partir de 1.400 distributeurs automatiques à travers le pays en seulement deux heures. Cette affaire intrigue sérieusement la police japonaise. Des malfaiteurs sont parvenus à voler 1,4 milliard de yens (11 millions d'euros) à partir de 1.400 distributeurs automatiques de billets différents. L'affaire était dans le sac en moins de deux heures.**

## Cartes contrefaites

Ce vol a probablement été mené par un groupe international faisant usage de cartes de crédit contrefaites contenant des informations de compte dérobées à une banque sud-africaine. Le nom de la banque n'a pas été mentionné et Interpol compte bien aider la police nippone dans cette affaire, comme le rapporte The Japan Times. 14.000 transactions Plus de 100 personnes pourraient avoir coordonné ce retrait d'argent colossal. Le montant maximal de 100.000 yen a été retiré dans chacune des 14.000 transactions…. [Lire la suite]

---

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

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

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

M

Réagissez à cet article

Source : *( Mobile ) – 11 millions volés dans une attaque simultanée de distributeurs automatiques*

---

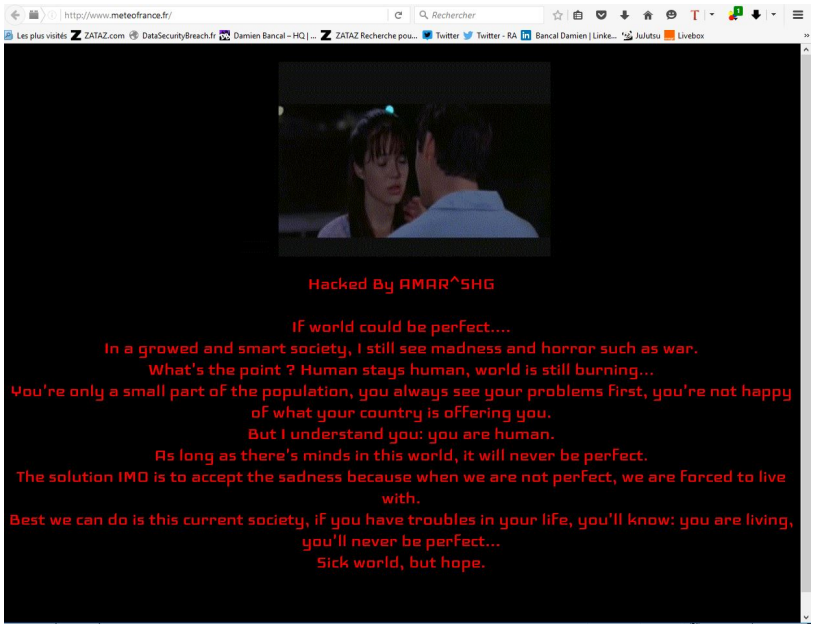
# Le site Internet de Météo France victime de détournement de DNS après celui de Canal +


M

Le site Internet de Météo France victime de détournement de DNS après celui de Canal +

---

**Après les sites de Canal +, un nouveau message d'espoir mis en ligne par un pirate informatique sur l'ensemble des sites Internet de Météo France. Un détournement de DNS radical.**




Il se nomme Amar^SHG. Ce jeune pirate informatique (Il serait un Albanais) est dans la mouvance des hacktivistes politiques qui, par le biais de la modification de site Internet (defacement, barbouillage), trouvent un moyen de faire passer des messages. Amar^SHG a fait la pluie et le beau temps sur les sites de Météo France via un détournement de DNS radical.
Lundi soir, le pirate a mis la main sur un moyen informatique qui lui a donné l'occasion de détourner l'ensemble des noms de domaines de Météo France. Comme il a pu me l'indiquer sur Twitter, les domaines .fr, .mobi, . Paris, … ont été impactés.

## Détournement de DNS

Les visiteurs accédaient, ce lundi soir (vers 22h30), à une page noire et rouge, portée par la musique « Wonderful life » de Katie Melua. Côté message, le cyber manifestant souhaitait viser ceux qui « se plaignent pour leurs propres problèmes ». AMAR ^ SHG parle d'espoir, d'un monde qui n'est pas parfait « Il faut vivre avec, avec espoir ».
Un message qui change des propos de haines, guerriers… que l'on peut croiser sur des pages modifiées par d'autres pirates informatiques. Une attaque qui a pu être mise en place via un phishing, un accès non autorisés à partir d'une injection SQL… Bref, plusieurs méthodes possibles ont pu être exploitées pour atteindre l'administration des noms de domaine et orchestrer ce détournement de DNS… [Lire la suite]

---



Réagissez à cet article

Source : *ZATAZ Détournement de DNS – Un pirate passe par Météo France – ZATAZ*

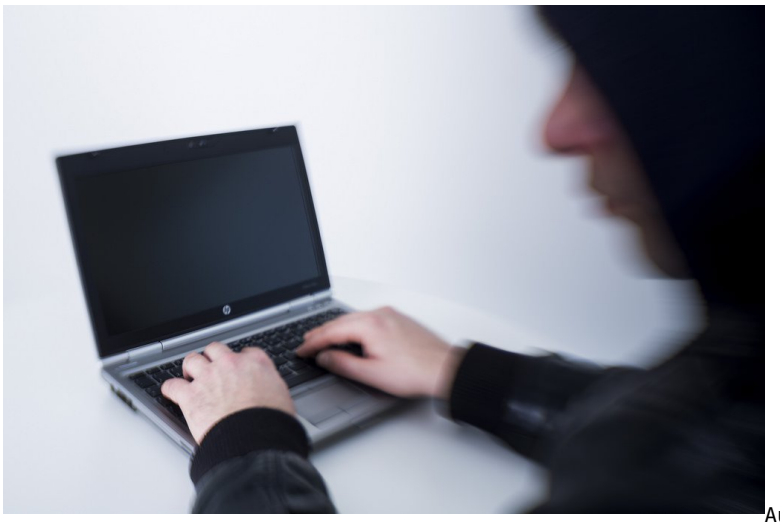
---

# La cybercriminalité fait des ravages dans les entreprises françaises.


La cybercriminalité fait des ravages dans les entreprises françaises

---

**Selon une étude du cabinet PwC, le nombre d'entreprises françaises victimes de la cybercriminalité a presque doublé en deux ans.**



Au cours des 2 dernières années, près de 70% des entreprises françaises ont été victimes de fraudes. On note notamment une forte hausse de la cybercriminalité, selon une étude effectuée par le cabinet Price Water House Coopers (PwC) publiée hier. La moyenne nationale est beaucoup plus élevée que celle mondiale.

**La cybercriminalité visant les entreprises françaises explose**

Les entreprises françaises sont-elles des cibles faciles pour les pirates ? Selon une étude de Price Water House Coopers concernant les fraudes en entreprises, les attaques informatiques occupent le deuxième rang derrière le détournement d'actifs. En 2 ans, la cybercriminalité a explosé en France, elle représente 53% des fraudes en 2016 contre 28% en 2014.

Aujourd'hui, une grande partie des entreprises (85%) ont pris conscience que le risque d'être victime de pirates informatiques est bel et bien réel. Elles n'étaient que 48% en 2014. Selon Louis Di Giovanni, travaillant dans le département Litiges et Investigations du cabinet PwC, « L'explosion du Big Data quels que soient les domaines, alliée à la digitalisation de l'activité économique et la multiplicité des supports numériques augmentent l'exposition des entreprises au risque de cyberattaque, d'où une plus grande prise en compte de ce risque par les dirigeants« .

**Les entreprises françaises ne sont pas prêtes face à ce risque**

Bien que les entreprises françaises aient bien pris en compte le risque élevé que représente la cybercriminalité, elles n'ont pas forcément mis en place de défenses adéquates. « Plus de la moitié des entreprises françaises n'ont pas encore de plan d'action 100% opérationnel pour répondre à une cyberattaque » déclarait M. Di Giovanni.

A cause de l'explosion de la cybercriminalité, le taux de fraude en entreprise progresse fortement. 68% des entreprises ont déclaré avoir été victimes d'une fraude au cours des deux dernières années, contre 55% en 2014, soit une hausse de 13 points… [Lire la suite]

L'étude PWC Global Economic Crime Survey 2016

---



Réagissez à cet article

Source : *La cybercriminalité fait des ravages dans les entreprises françaises*

Auteur : David Pain