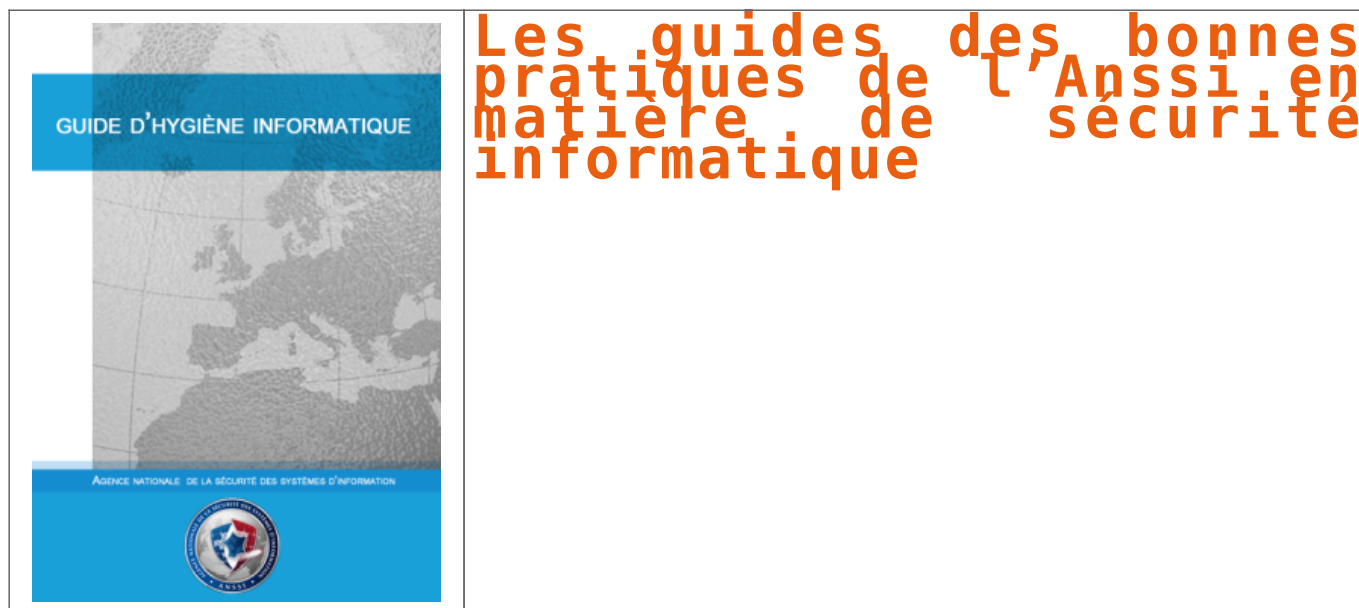


# Les guides des bonnes pratiques de l'Anssi en matière de sécurité informatique | Denis JACOPINI



**Vous voulez éviter que le parc informatique soit utilisé pour affaiblir votre organisation ? L'un des guides publiés par l'ANSSI vous aidera à vous protéger.**

Initialement destinés aux professionnels de la sécurité informatique, les guides et recommandations de l'ANSSI constituent des bases méthodologiques utiles à tous. Vous trouverez sans peine votre chemin en utilisant les mots-clés, qu'un glossaire vous permet d'affiner, ou le menu thématique.

#### LISTE DES GUIDES DISPONIBLES

- Guide pour une formation sur la cybersécurité des systèmes industriels
- Profils de protection pour les systèmes industriels
- Sécuriser l'administration des systèmes d'information
- Achat de produits de sécurité et de services de confiance qualifiés dans le cadre du rgs
- Recommandations pour le déploiement sécurisé du navigateur mozilla firefox sous windows
- Cryptographie – les règles du rgs
- Recommandations de sécurité concernant l'analyse des flux https
- Partir en mission avec son téléphone sa tablette ou son ordinateur portable
- Recommandations de sécurité relatives à active directory
- Recommandations pour le déploiement sécurisé du navigateur microsoft internet explorer
- l'homologation de sécurité en neuf étapes simples,
- bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine,
- recommandations pour le déploiement sécurisé du navigateur google chrome sous windows,
- usage sécurisé d'(open)ssh,
- la cybersécurité des systèmes industriels,
- sécuriser une architecture de téléphonie sur ip,
- mettre en œuvre une politique de restrictions logicielles sous windows,
- prérequis à la mise en œuvre d'un système de journalisation,
- vulnérabilités 0-day, prévention et bonnes pratiques,
- le guide des bonnes pratiques de configuration de bgp,
- sécuriser son ordiphone,
- sécuriser un site web,
- sécuriser un environnement d'exécution java sous windows,
- définition d'une politique de pare-feu,
- sécuriser les accès wi-fi,
- sécuriser vos dispositifs de vidéoprotection,
- guide d'hygiène informatique,
- la sécurité des technologies sans contact pour le contrôle des accès physiques,
- recommandations de sécurité relatives à ipsec,
- la télé-assistance sécurisée,
- sécurité des systèmes de virtualisation,
- sécurité des mots de passe,
- définition d'une architecture de passerelle d'interconnexion sécurisée,
- ebios – expression des besoins et identification des objectifs de sécurité,
- la défense en profondeur appliquée aux systèmes d'information,
- externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques,
- archivage électronique... comment le sécuriser ?
- pssi – guide d'élaboration de politiques de sécurité des systèmes d'information,
- tdbssi – guide d'élaboration de tableaux de bord de sécurité des systèmes d'information,
- guide relatif à la maturité ssi,
- gissip – guide d'intégration de la sécurité des systèmes d'information dans les projets

---

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.ssi.gouv.fr/entreprise/bonnes-pratiques/>

---

# Attaque informatique : les 7 gestes qui sauvent



## Attaque informatique : les 7 gestes qui sauvent

---

Perspectives IT, 14 octobre 2016, 11:00SÉCURITÉ 3 1 10BLOG PROPOSÉ PAR DELL EMCVotre PC est infecté. Mais repérer l'attaque n'est que la première étape. Il faut ensuite organiser la réponse à incident. Et les premiers gestes ont ici une importance capitale.

7 gestes de premiers secours à connaître face à une attaque informatique. Votre poste de travail est infecté. La stratégie en place de détection des intrusions a fonctionné et une menace a été identifiée. Et ensuite ? Repérer l'attaque informatique n'est que la première étape. Encore faut-il savoir ensuite organiser la réponse à incident. Et les premiers gestes ont ici une importance capitale. Pour éviter que la situation ne s'aggrave tout d'abord, mais aussi pour permettre de récolter un maximum d'informations sur l'attaque. Les collaborateurs d'une entreprise n'étant pas censés être tous des experts en sécurité informatique, la formation et la sensibilisation sont des missions clés des RSSI. Pour les aider, le CERT-FR a dressé une liste des bons réflexes à adopter.



---

**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>



Réagissez à cet article

Source : *Attaque informatique : les 7 gestes qui sauvent – Silicon*

---

# Attaques informatiques : Comment s'en protéger ?

x	Attaques informatiques : Comment s'en protéger ?
---	---

---

**Les cyberattaques se faisant de plus en plus nombreuses et sévères, les entreprises doivent apprendre à s'en protéger. Pour cela, les directions juridiques et de l'informatique peuvent s'appuyer sur l'expertise de la police judiciaire et des experts en data protection.**

Tous les quinze jours en moyenne, une attaque sévère – où des données sont exfiltrées – est découverte. Face à ce constat, le tribunal de commerce de Paris a réuni quatre tables rondes d'experts de la sécurité informatique, des représentants de la police judiciaire et des experts-comptables fin juin pour examiner les solutions de protection dont disposent les entreprises. Julien Robert, directeur de la sécurité chez SFR, résume les trois facteurs agissant sur la sécurité : les utilisateurs, car ce sont eux qui choisissent les données qu'ils utilisent et partagent, les fournisseurs d'accès et l'encadrement d'un data center externe fortement conseillé.

#### **Prévention**

« *Il est difficile d'agir lorsque l'attaque a déjà eu lieu* », précise Sylvie Sanchis, chef de la Befiti (1) de la police judiciaire de Paris. Le moyen le plus efficace dont disposent les entreprises pour se protéger est donc la prévention. Il faut avant tout investir dans la sécurité informatique. Si certaines sociétés sont réticentes en raison du coût, il est important de rappeler qu'il sera toujours moindre que celui engendré par une attaque.

Tous les salariés doivent par ailleurs être formés car certaines intrusions sont rendues possibles par leur comportement, sans qu'ils en soient conscients, notamment par leur exposition sur Internet.

#### **Les modes opératoires**

Les modes opératoires d'exfiltration des données se diversifient et se sophistiquent au fil des années. Certains se veulent discrets afin que l'entreprise ne prenne connaissance de l'attaque que très tardivement, d'autres relèvent du chantage ou de la demande de rançon.

L'attaque peut venir d'un mail qui, à son ouverture, téléchargera un virus sur l'ordinateur de l'employé. Les données peuvent également être extraites grâce au social engineering, pratique qui exploite les failles humaines et sociales de la cible, utilisant notamment la crédulité de cette dernière pour parvenir à ses fins (arnaque au patron). Quant aux ransomwares, il s'agit de logiciels malveillants permettant de rançonner l'entreprise pour qu'elle récupère ses données. Dans ce cas, Anne Souvira, chargée de mission aux questions liées à la cybercriminalité au cabinet du préfet de police de Paris, précise que « *même si l'entreprise paye, il est très rare de récupérer toutes les données.* » Si elle peut être tentée de payer la rançon sans prévenir les autorités compétentes pour une somme modique, il n'y a aucune garantie de récupérer les données et les traces de l'attaque seront perdues. D'autres techniques de chantage sont utilisées, comme lorsque l'on se voit menacer d'une divulgation des vulnérabilités du système.

#### **L'importance de porter plainte**

La réaction à adopter, la plus rapide possible, fait partie de la sécurité informatique : « *C'est un travail de réflexion en amont qui permettra d'adopter la bonne stratégie* », selon Cirył Piat, lieutenant-colonel de la gendarmerie nationale. Suite à une cyber-attaque, la plupart des entreprises sont réticentes à porter plainte, par peur d'une mauvaise réputation ou par scepticisme vis-à-vis de la réelle utilité de cette procédure. Alice Cherif, chef de la section « cybercriminalité » du parquet de Paris, précise que la plainte présente l'avantage d'identifier les éléments d'investigation qui permettront de remonter au cybercriminel. « *Toute autre alternative est bien moins efficace et fait perdre un temps précieux à l'entreprise ainsi que des éléments d'investigation.* »

#### **L'utilité du cloud**

L'une des façons de sécuriser ses données est de les confier à un tiers spécialiste qui les stockera en ligne sur un cloud. « *Il s'agit d'un système complexe connecté sur Internet, où les données sont stockées sur des disques durs physiques situés dans des salles d'hébergement, les fameux data centers* », explique Julien Levrard, chef de projet sécurité chez OVH. Le cloud rend l'accès plus difficile aux malfaiteurs d'autant qu'ils ignorent la localisation de la donnée. Vigilance et prévention : les maîtres mots en matière de cybercriminalité.

Article original de Emilie Smelten

(1) Brigade d'enquête sur les fraudes aux technologies de de l'information



Réagissez à cet article

**Original de l'article mis en page : Cybercriminalité : comment se protéger ? – Magazine Decideurs**

---

# LeNetExpert a intégré la plateforme cybermalveillance.gouv.fr

Notre métier en RGPD et en CYBER : Auditer, Expertiser,  
Accompagner, Former et Informer



**LeNetExpert a intégré la  
plateforme  
cybermalveillance.gouv.fr**

**Parce que les victimes doivent pouvoir compter sur des professionnels habitués à réagir face à des actes de piratage, des escroqueries ou vols de données etc., nous avons tenu à soutenir le projet cybermalveillance.gouv.fr. à mettant à leur disposition le meilleur de nos compétences.**

2017 sera probablement l'année qui comptera le plus de victimes de rançongiciels. Les initiatives que l'on peut identifier sur le cyberspace ayant pour objectif de combattre ce fléau démontrent une réelle prise de conscience à toutes les strates de l'économie et de l'état. Vous trouverez ci-dessous un guide pdf spécialement fait pour vous aider à anticiper et à réagir face de telles menaces. Cette fiche réflexe est destinée à toutes les catégories de publics. Elle présente cette catégorie d'attaque informatique, les principales mesures à prendre pour s'en protéger, les actions à entreprendre lorsque l'on en est victime, ainsi que les infractions et sanctions pénales auxquelles s'exposent ceux qui les utilisent.



**RÉPUBLIQUE  
FRANÇAISE**

*Liberté  
Égalité  
Fraternité*

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).

---

#### LE NET EXPERT

:

- **SENSIBILISATION / FORMATIONS :**
    - **CYBERCRIMINALITÉ**
    - **PROTECTION DES DONNÉES PERSONNELLES**
      - AU RGPD
      - À LA FONCTION DE DPO
    - **MISE EN CONFORMITÉ RGPD / CNIL**
      - ÉTAT DES LIEUX RGPD de vos traitements
      - MISE EN CONFORMITÉ RGPD de vos traitements
      - SUIVI de l'évolution de vos traitements
    - **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**

Réagissez à cet article

Source : *Fiche rançongiciels (cryptolocker)*

**52 % des entreprises ont  
indiqué avoir subi un  
rançongiciel « majeur » dans  
les 12 derniers mois**

Notre métier en RGPD et en CYBER : Auditer, Expertiser,  
Accompagner, Former et Informer



**52 % des  
entreprises ont  
indiqué avoir subi  
un rançongiciel  
« majeur » dans  
les 12 derniers  
mois**



En France, 52 % des entreprises ont indiqué avoir subi un rançongiciel « majeur » dans les 12 derniers mois. Elles étaient 48 % en 2019. Le coût moyen d'une attaque par rançongiciel est de 420 000 euros en dehors de la rançon exigée. Ce montant prend en compte les temps d'arrêt, la perte de chiffre d'affaires et les coûts opérationnels. En cas de paiement de la rançon, cette somme double.



### **LA CLÉ DE CHIFFREMENT N'EST PAS UNE SOLUTION MIRACLE**

*« Les entreprises se sentent parfois sous pression pour payer la rançon afin d'éviter les temps d'arrêt préjudiciables. À première vue, effectuer le paiement de la rançon semble être une manière efficace de restaurer les données, mais ce n'est qu'illusoire (...) En effet, une simple clé de chiffrement n'est pas un remède miracle et il faut souvent bien plus pour restaurer les données »*, a expliqué Chester Wisniewski, Principal Research Scientist chez Sophos.

En France, plus de la moitié (61%) des responsables IT interrogés déclarent avoir pu restaurer leurs données à partir de sauvegardes sans payer la rançon. Dans 2 % de cas, le paiement de la rançon n'a pas permis de restaurer les données. À l'échelle mondiale, ce chiffre s'élève à 5 % pour les organisations du secteur public.

...[lire la suite]

### **Commentaire de notre Expert : Denis JACOPINI**

La demande de rançon est la résultante dans la quasi totalité des cas de l'ouverture d'une pièce jointe à e-mail piégé ou le clic sur un lien aboutissant sur un site Internet piégé.

#### Les conséquences

Il n'est plus à rappeler qu'être victime d'un ransomware entraîne un arrêt de l'outil informatique, une perte de productivité et une dégradation de la réputation auprès des clients et partenaires.

#### Les solutions

Nous le répéterons jamais assez, les seuls moyens d'empêcher ce type de situation sont l'utilisations d'outils de filtrage et la sensibilisation. N'hésitez pas à nous contacter pour l'organisation de sessions de sensibilisation auprès de vos équipes pour leur apprendre à détecter e-mails et sites Internet malveillants, en quasi totalité à l'origine des rançongiciels dans les systèmes informatiques.

---

Réagissez à cet article

**Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :**

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

**Quel est notre métier ?**

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques.**

**Quel sont nos principales activités ?**

▪ **RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

▪ **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique 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).

*« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et*

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.

Denis JACOPINI »

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

---

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



- Mises 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, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)



Source : Etude : Payer la rançon multiplie par deux le coût total d'un ransomware

# Des pirates informatiques profitent du coronavirus pour vous piéger et vous infecter avec un virus

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



Des pirates informatiques profitent du coronavirus pour vous piéger et vous infecter avec un virus

**Les courriels – qui circulent principalement en Asie pour le moment – prétendent contenir de l’information légitime au sujet du coronavirus.**

Le destinataire est invité à cliquer sur une pièce jointe pour obtenir plus d’information. Ceux qui tombent dans le piège permettent involontairement aux pirates d’avoir accès à leurs documents personnels.

IBM dit qu’on s’attend à «voir circuler davantage de courriels malveillants inspirés par le coronavirus dans le futur, alors que l’infection se propagera. Cela se produira probablement aussi dans d’autres langues».

Les pirates informatiques exploitent régulièrement l’actualité et les craintes de la population pour sévir. «Une telle stratégie permet de berner plus de victimes pour qu’elles cliquent des liens malveillants ou ouvrent des fichiers malveillants, accroissant ultimement l’efficacité de la campagne malveillante», peut-on lire dans le rapport...[lire la suite]

---

Réagissez à cet article

**Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :**

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

**Quel est notre métier ?**

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques.**

**Quel sont nos principales activités ?**

▪ **RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

▪ **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique 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).

*« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et*

*les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.*

*Denis JACOPINI »*

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

---

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



- Mises 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, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)



Source : *Des pirates informatiques profitent du coronavirus pour répandre un logiciel malveillant | HuffPost Québec*



---

# Envoyé spécial sur les Cyberattaques : les braqueurs de l'ombre – 14 décembre 2017 (France 2)



Envoyé spécial  
sur les  
Cyberattaques  
: les  
braqueurs de  
l'ombre – 14  
décembre 2017  
(France 2)

**Les hold-up 2.0 par des « rançongiciels », logiciels de rançon, se multiplient : en France, une entreprise sur deux aurait déjà été piratée de cette façon. Enquête du magazine « Envoyé spécial » sur un fléau invisible en pleine explosion.**

Merci à Clément Le Goff et Guillaume Beaufiles pour ce beau travail d'enquête. Tout est vrai, et encore, tout n'est pas dit. Quelles conséquences avec les objets connectés, bientôt principaux cadeaux de Noël, les voitures connectées, et tous les outils informatiques ou algorithmiques dont leurs usages peuvent être détournés à des fins malveillantes.

Depuis plusieurs années, Denis JACOPINI essaie par le biais de conférences ou en participant à des émissions de radio ou de TV (D8, LCI, NRJ12, Sud Radio, Sputnik...) de sensibiliser la population à ces risques afin de les aider à anticiper et éviter le plus possible ces attaques en leur apprenant à se protéger des pirates informatiques.

Avec un tel reportage, j'espère que le plus grand nombre de personnes sera sensibilisé de manière à enrayer ce phénomène incoercible.

Seul petit bémol dans ce reportage. Beaucoup auront entendu et retenu les recommandations de la police qui sont qu'il ne faut pas payer la rançon lorsqu'un pirate prend vos données en otage. Je compléterais par le fait qu'il ne faut pas payer si vous avez la possibilité d'utiliser des sauvegardes ou si les conséquences sont minimales. Par contre, si la vie d'une entreprise est en jeu et la seule chance restante (même infime) pour sauver l'entreprise est de payer la rançon, ne pas la payer risquerait bien de vous être reproché... à moins que ça soit, comme dans le reportage un coup de grâce accepté par désespoir.

Corriger le message afin de ne pas induire les entreprises en erreur me paraît indispensable.

---

#### 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).



Réagissez à cet article

**Les hold-up 2.0 par des « rançongiciels », logiciels de rançon, se multiplient : en France, une entreprise sur deux aurait déjà été piratée de cette façon. Enquête du magazine « Envoyé spécial » sur un fléau invisible en pleine explosion.**

Depuis plusieurs années, Denis JACOPINI essaie par le biais de conférences ou en participant à des émissions de radio ou de TV (D8, LCI, NRJ12, Sud Radio, Sputnik) de sensibiliser la population à ces risques afin de les aider à anticiper et éviter ces attaques.

Merci à *Clément Le Goff et Guillaume Beaufile*  
Avec un tel reportage, j'espère que

---

#### 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).



Réagissez à cet article

---

# Alerte Android : Le pire ransomware jamais détecté fait ses premières victimes

✕	Alerte Android : Le pire ransomware jamais détecté fait ses premières victimes
---	--

---

Android est à nouveau visé par un malware vendredi 13 octobre : DoubleLocker, un redoutable ransomware, chiffre les fichiers sur le smartphone et change son mot de passe, même s'il n'est pas rooté. Des chercheurs de ESET à l'origine de la découverte expliquent que ce ransomware se cache dans un APK d'Adobe Flash Player ce qui peut augmenter le risque d'une propagation rapide. La seule façon de s'en débarrasser c'est de réinitialiser le smartphone. Ce serait le pire ransomware détecté à ce jour.

Les chercheurs de ESET viennent de découvrir le premier ransomware Android capable de prendre le contrôle total de votre smartphone. Il parvient à obtenir des droits administrateur même sur des smartphone non-rootés, ce qui le rend extrêmement dangereux. Android/DoubleLocker.A est basé sur un trojan bancaire modifié pour changer le code PIN du smartphone sur lequel il est installé et chiffrer ses données. Les chercheurs précisent qu'un tel mode d'action était jusqu'ici du jamais vu.

## Android : le pire ransomware jamais détecté, DoubleLocker, bloque et chiffre les smartphones

Le chercheur Lukáš Štefanko à l'origine de la découverte de DoubleLocker ajoute : « à cause du fait qu'il trouve son origine dans un malware bancaire, DoubleLocker pourrait très bien être modifié pour devenir ce que l'on pourrait appeler un malware bancaire-rançon. Un malware à deux étages, qui essaie d'abord de voler vos données bancaires et/ou vider votre compte ou compte PayPal, puis bloque votre appareil et ses données pour exiger une rançon... spéculation de côté, on a détecté la version test d'un tel malware dans la nature pratiquement en même temps, en mai 2017 ». On trouve DoubleLocker dans des APK de Flash Player sur de sites compromis méthode déjà utilisée par d'autres malwares. Une fois lancée, l'application lance un service d'accessibilité baptisé Google Play Service. Le malware obtient ensuite tout seul les permissions d'accessibilité, puis les utilise pour activer les droits administrateurs et se définir comme *Launcher* par défaut. Dès que l'utilisateur appuie sur le bouton Home, le malware est activé. Le PIN est alors changé et les fichiers du répertoire principal chiffrés. Le ransomware demande alors de payer 0.013 BTC dans les 24 heures, soit environ 62 euros au moment où nous écrivons ces lignes. Les chercheurs relèvent que les fichiers chiffrés, qui prennent l'extension .cryeye, ne sont pas supprimés à l'issue de ce délai...[lire la suite]

---

QUE PROPOSE LE NET EXPERT, (EXPERT INFORMATIQUE ASSERMENTÉ) :

- SENSIBILISATIONS / FORMATIONS (n° formateur)
  - RECHERCHE DE PREUVES
- EXPERTISES & AUDITS (certifié ISO 27005)  
NOTRE MÉTIER :
  - SENSIBILISATION / FORMATIONS :
    - 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

**FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO** : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, suivez nos formations ;

**COLLECTE & RECHERCHE DE PREUVES** : Nous mettrons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

**EXPERTISES TECHNIQUES** : Dans le but de prouver un dysfonctionnement, de déposer ou vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

**AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT** : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des nombreuses formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration et vous accompagnons dans l'établissement d'une analyse d'impact et de votre mise en conformité ;

**MISE EN CONFORMITÉ CNIL/RGPD** : Nous mettrons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assisterons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

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

**NOS FORMATIONS** : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>  
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Android : le pire ransomware jamais détecté fait ses*

# **Alerte ! LeakerLocker : un nouveau logiciel de rançon se manifeste sur Android**

	<b>Alerte ! LeakerLocker : un nouveau logiciel de rançon se manifeste sur Android</b>
---	---

---

**Android doit faire face à un nouveau ransomware qui menace de dévoiler des informations compromettantes sur l'utilisateur du smartphone.**

Android est le système d'exploitation le plus utilisé. Il est donc la cible de nombreux logiciels malveillants, c'est le cas de LeakerLocker. **Ce dernier est un ransomware, autrement dit un logiciel de rançon qui récupère des informations personnelles, menaçant de dévoiler leurs contenus si une certaine somme d'argent ne lui est pas versée.** LeakerLocker, quant à lui est un logiciel de rançon qui promet de vous humilier. **Pour cela, il utilise les données de votre historique de recherches et menace de l'envoyer à vos contacts.** Le montant de la rançon s'élève à 50 euros. Un logiciel de rançon d'un nouveau genre fait son apparition sur Android.

## **Un logiciel de rançon apparu en premier lieu sur Android**

McAfee, le logiciel antivirus stipule que ce logiciel malveillant est né sur le système d'exploitation Android. **Il se propage avec l'installation de deux applications disponible sur Google Play : Booster & CCleaner Pro ainsi que Wallpapers Blur HD.** Il réussit à dérober des informations qui pourraient vous nuire, au sein de votre smartphone afin de les utiliser contre vous...[lire la suite]

---

### **NOTRE MÉTIER :**

**PRÉVENTION** : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

**RÉPONSE A INCIDENTS** : Vous aider à rechercher l'origine d'une attaque informatique, recueillir les preuves pour une utilisation auprès de la justice ou des assurances, identifier les failles existantes dans les systèmes informatiques et améliorer la sécurité de l'existant ;

**SUPERVISION** : Assurer le suivi de la sécurité de votre installation pour la conserver le plus possible en concordance avec l'évolution des menaces informatiques.

**MISE EN CONFORMITÉ CNIL** : Vous assister dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

**Besoin d'un Expert ? contactez-vous**

#### **NOS FORMATIONS**

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>  
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *LeakerLocker : un nouveau logiciel de rançon se manifeste sur Android*

---

# Les points faibles du Ransomware Petya/NotPetya



## Les points faibles du Ransomware Petya/NotPetya

Alors que le mystère s'épaissit sur les intentions réelles des auteurs du malware parti d'Ukraine fin juin, des chercheurs d'une société de sécurité informatique britannique sont parvenus à décrypter des fichiers endommagés sur une machine infectée.

Jusqu'à présent, toutes les actions entreprises pour récupérer les données attaquées par NotPetya sont vouées à l'échec.

### Erreur de programmation de l'algorithme de cryptage

Un maigre espoir pour les victimes du malware Petya/NotPetya : sur leur blog les chercheurs en cybersécurité de la société britannique Positive Technologies expliquent avoir réussi à décrypter des fichiers endommagés sur un ordinateur infecté. Très ardue, la procédure de récupération ne serait possible que sur certaines machines, celles dont le virus a encrypté les droits d'administrateur. Une découverte fort intéressante, alors que jusqu'à présent, personne, y compris les victimes ayant payé la rançon exigée par les attaquants, n'a pu récupérer ses données...

Positive Technologies a découvert plusieurs erreurs commises par les pirates dans la conception du malware, en particulier dans la programmation de l'algorithme de cryptage Salsa20. Au lieu d'utiliser une clé de chiffrement de 256 bits, ils se sont apparemment contentés d'une clé moins puissante de 128 bits, que Positive Technologies est parvenu à contourner pour récupérer certains fichiers...[lire la suite]

**Notre métier** : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec le RGPD (règlement Européen relatif 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>



Réagissez à cet article

Source : *Petya/NotPetya : des chercheurs ont découvert des points faibles*