

# Autonomie des laptops : les mensonges des industriels démontrés par une étude



A l'instar des volumes de consommation d'essence et d'émanation de CO2 des voitures, l'autonomie des laptop atteint rarement les belles promesses affichées par le constructeur...[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 de formation, de sensibilisation ou d'audits 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 sur cette page.

---



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

---

## Autonomie des laptops : les mensonges des industriels démontrés par une étude



A l'instar des volumes de consommation d'essence et d'émanation de CO2 des voitures, l'autonomie des laptop atteint rarement les belles promesses affichées par le constructeur...[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 de formation, de sensibilisation ou d'audits 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 sur cette page.

---



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

# Découvrez comment supprimer le ransomware WannaCry, sans payer la rançon



Découvrez comment supprimer le ransomware WannaCry, sans payer la rançon

La ransomware WannaCry est toujours d'actualité, bien que Microsoft ait déployé les correctifs il y a quelques jours maintenant. Certains utilisateurs ne les ont pas encore appliqués et d'autres ont été infectés avant la diffusion. Bonne nouvelle cependant, il est possible de retirer WannaCry et donc d'avoir de nouveau accès aux fichiers de son ordinateur sans payer la rançon demandée (300 dollars).

Avant de commencer, il est bon de préciser qu'il est nécessaire de ne pas avoir redémarré ou éteint son ordinateur depuis qu'il a été infecté. Si c'est le cas, la solution tombe à l'eau malheureusement. Mais pour les autres, la solution s'appelle **Wanakiwi** et a été développée par des Français, à savoir Benjamin Delpy, Adrien Guinet et Matthieu Suiche.

Comment fonctionne Wanakiwi ? Il se charge d'analyser la mémoire du PC parce que la clé de déchiffrement s'est inscrite brièvement dans celle-ci. L'outil va alors tenter de la retrouver pour déchiffrer tous les documents qui sont verrouillés sur l'ordinateur par WannaCry. L'opération prend quelques minutes. Elle fonctionne aussi bien sur Windows XP que sur Windows 7. Cela devrait aussi fonctionner sur Windows Vista, mais un test n'a pas été réalisé.

Pour utiliser Wanakiwi, il faut télécharger la version la plus récente (wanakiwi\_0.2.zip pour l'instant) sur GitHub, dézipper l'archive, lancer l'invité de commande sur Windows en mode administrateur et ouvrir le fichier wanakiwi.exe depuis l'invité de commande. Le travail va alors s'effectuer automatiquement. Il est possible de s'aider de cette vidéo si besoin.

---

**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 : *Il est possible de supprimer le ransomware WannaCry,*

**Voici deux outils permettant  
de lutter contre les  
épidémies récentes de  
ransomwares dont WannaCry**





**ESET® annonce la publication d'un outil de contrôle de la vulnérabilité EternalBlue et une clé de déchiffrement pour les variantes de Crysis. Ces deux outils, mis au point par les chercheurs ESET, permettent aux entreprises une mise à jour efficace suite aux récentes cyberattaques.**

Le premier outil vérifie si Windows® est protégé contre l'exploit EternalBlue, responsable en partie de l'attaque WannaCry. Ce dernier est d'ailleurs toujours utilisé pour diffuser entre autres des logiciels de cryptomonnaie. L'exploit EternalBlue (CVE-2017-0144) détecté par ESET a été ajouté le 25 avril 2017 avant son exploitation par la menace WannaCry.

Le deuxième outil publié par ESET permet le déchiffrement et s'adresse aux victimes de l'une des variantes du ransomware Crysis, qui utilise comme extension pour les fichiers chiffrés .wallet et .onion. Les clés ont été publiées le 18 mai sur les forums de BleepingComputer.com.

Les deux outils sont disponibles en téléchargement à partir de la page Internet d'ESET :

- Vérificateur de la vulnérabilité EternalBlue : [https://help.eset.com/eset\\_tools/ESETeternalBlueChecker.exe](https://help.eset.com/eset_tools/ESETeternalBlueChecker.exe)
- Clé de déchiffrement du ransomware Crysis .wallet / .on : <https://download.eset.com/com/eset/tools/decryptors/crysis/latest/esetcrysisdecryptor.exe>

**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 : ESET

---

# WannaCry : seulement trois antivirus protègent de l'exploit EternalBlue

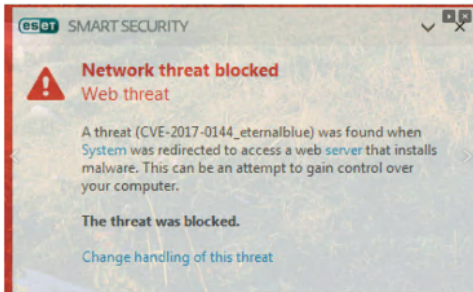


WannaCry :  
seulement  
trois  
antivirus  
protègent  
de  
l'exploit  
EternalBlue



**Prompts à clamer qu'ils bloquent WannaCry, les éditeurs d'antivirus oublient de mentionner qu'ils ne détectent pas, à trois exceptions près, l'exploit EternalBlue. Or, c'est celui-ci qui risque d'être réutilisé par de nouvelles menaces.**

Depuis la crise WannaCry, qui s'est déclenchée le 12 mai 2017 et s'est traduite par l'infection de centaines de milliers de systèmes, les éditeurs d'antivirus n'hésitent pas à clamer que leurs outils arrêtent tous la menace. Un test monté par MRG Effitas, une entreprise anglaise spécialisée dans la recherche en sécurité informatique (MRG signifiant Malware Research Group), montre que la réalité est un peu plus contrastée.



En testant la capacité des logiciels de protection grand public (avec leurs paramètres par défaut) à détecter l'exploit EternalBlue, mis à profit par WannaCry pour se diffuser, MRG Effitas établit que seuls trois produits stoppent le code de la NSA récupéré par les auteurs du ransomware : Eset Smart Security, F-Secure Safe et Kaspersky Internet Security. « Deux de ces produits utilisent le filtrage réseau pour détecter cet exploit et le bloquer avant son exécution au niveau du noyau », écrit MRG Effitas, qui précise que ce mode de détection pourrait être contourné en masquant la signature de l'exploit.  
..[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 : WannaCry : seulement trois antivirus protègent de l'exploit EternalBlue

---

# Cyberattaque : va-t-on un jour prendre votre télévision connectée en otage ?



Cyberattaque :  
va-t-on un  
jour prendre  
votre  
télévision  
connectée en  
otage ?

**Pour exiger une rançon, des hackers pourraient pirater vos cafetières, télévisions, GPS connectés. Mais est-ce vraiment crédible ?**

Les récentes attaques massives de « ransomwares », ces logiciels malveillants exigeant une rançon pour débloquer les ordinateurs qu'ils ont infectés, font craindre pour l'avenir des objets connectés, **des jouets aux téléviseurs en passant par le réfrigérateur ou la cafetière**, qui se multiplient dans nos foyers.

« Concernant l'attaque du week-end passé, il n'y a pas de risque pour les objets connectés. Elle touchait en particulier des systèmes avec Windows (...), et il n'y a pas d'objets connectés grand public aujourd'hui qui embarquent Windows pour fonctionner », assure G r me Billois, consultant chez Wavestone. « En revanche, il y a **d j  eu des attaques massives sur des objets connect s** », rappelle-t-il.

Le malware (logiciel malveillant) Mirai a ainsi r cemment infect  par centaines de milliers des objets connect s mal s curis s, non pas pour les bloquer, mais **pour les transformer en zombies et cr er des relais pour de futures cyberattaques**.

## Transformer vos objets en mouchards

Mardi   La Haye, le jeune prodige Reuben Paul, 11 ans, a  pat  une galerie d'experts en cybers curit  en piratant le bluetooth de leurs appareils  lectroniques pour prendre le contr le d'un ours en peluche.

Les objets connect s sont donc des cibles tout   fait cr dibles, qui peuvent aussi bien **siphonner des donn es** que se **transformer en mouchards**. Selon des documents r v l s en mars par Wikileaks, les services de renseignement am ricains sont capables de « hacker » des smartphones, des ordinateurs et des t l visions intelligentes, notamment pour prendre **le contr le de leurs micros et  couter ce qu'il se passe**.

*« Tous les autres objets connect s sont piratables,  a a  t  d montr , que ce soit la cafeti re, le r frig rateur, le thermostat, la serrure  lectronique, le syst me d' clairage... »*Lo c Gu zo strat giste cybers curit 

*...[lire la suite]*

---

**Notre m tier :** Vous aider   vous prot ger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos d marches de mise en conformit  avec la r glementation relative   la protection des donn es   caract re personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et   l' tranger, nous r pondons aux pr occupations des d cideurs et des utilisateurs en mati re de cybers curit  et de mise en conformit  avec le r glement Europ en relatif   la Protection des Donn es   caract re personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libert s (CIL) ou d'un Data Protection Officer (DPO) dans votre  tablissement.. (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 sp cialis  en « S curit  » « Cybercriminalit  » et en protection des « Donn es   Caract re Personnel ».

- Audits S curit  (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves t l phones, disques durs, e-mails, contentieux, d tournements de client le...);
- Expertises de syst mes de vote  lectronique ;
- Formations et conf rences en cybercriminalit  ;  
(Autorisation de la D TEF n 93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libert s) ;
- Accompagnement   la mise en conformit  CNIL de votre  tablissement.



[Contactez-nous](#)



R agissez   cet article

Source : *Cyberattaque : va-t-on un jour prendre votre télévision connectée en otage ? – Sud Ouest.fr*

---

# Cyberattaque mondiale : trois Français ont créé un logiciel anti WannaCry



**What Happened to My Computer?**  
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**  
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**  
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

**Send \$300 worth of bitcoin to this address:**  
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Cyberattaque mondiale : trois Français ont créé un logiciel anti WannaCry

---

**Il s'appelle WannaKiwi, et peut éviter le verrouillage de fichiers, mais il faut l'utiliser de tout urgence, selon ses inventeurs français**

Cocorico ! Un groupe de trois Français, experts en sécurité informatique, a annoncé ce vendredi avoir mis au point un logiciel qu'ils ont nommé WannaKiwi permettant de récupérer les documents Windows cryptés par le virus informatique WannaCry, lors d'une cyberattaque massive.

« Rançongiciel », WannaCry a infecté quelque 300 000 ordinateurs dans plus de 150 pays la semaine dernière. En France, c'est principalement le groupe automobile Renault qui a été affecté, avec le blocage de chaînes de production. Une fois implanté, ce logiciel malveillant, qui utilise une faille de Windows, paralyse le système informatique en cryptant les données. Pour récupérer ces fichiers, il faut un code que les pirates fournissent (ou pas) en échange d'une rançon.

.../...

Pour télécharger WannaKiwi : <https://github.com/gentilkiwi/wanakiwi/releases>

Pour voir le blog d'informations (en anglais) : <https://blog.comae.io/wannacry-decrypting-files-with-wanakiwi-demo-86bafb81112d>

---

**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 : *Cyberattaque : trois Français ont créé un logiciel*







**Cette nouvelle cyberattaque, plus discrète que WannaCry serait en action depuis début mai 2017. Elle se servirait de la même faille dans le système informatique Windows pour s'infiltrer dans les données des ordinateurs.**

Adylkuzz opère de façon plus invisible en créant une monnaie virtuelle dans l'ordinateur infecté avant d'envoyer cet argent à des adresses cryptées, volant les utilisateurs sans laisser de traces et sans qu'ils ne s'en aperçoivent.

« Bien que plus silencieuse et sans interface utilisateur, l'attaque d'Adylkuzz est plus rentable pour les cybercriminels. Elle transforme les utilisateurs infectés en participants involontaires au financement de leurs assaillants », explique Nicolas Godier, un expert en cyber sécurité de Proofpoint à l'AFP.

Le seul effet secondaire de ce virus est un ralentissement des performances de l'ordinateur infecté. Il est donc très difficile à diagnostiquer. Adylkuzz ferait aujourd'hui des centaines de milliers de victimes, et les sommes volées sont beaucoup plus importantes que celles de WannaCry.

---

**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 : *WannaCry: malgré un ralentissement de l'infection, la cyberattaque reste inquiétante*

---

# Des hackers à l'origine de la cyber attaque mondiale menacent de divulguer d'autres failles



Des  
hackers à  
l'origine de  
la  
cyber  
attaque  
mondiale  
menacent  
de  
divulguer  
d'autres  
failles

**Le groupe de pirates Shadow Brokers, qui avaient révélé la faille du système Windows à l'origine de la vaste opération de cyberattaque, affirme dans un message qu'il pourrait récidiver.**

Le mystérieux groupe de pirates informatiques Shadow Brokers, qui a révélé en avril la faille exploitée pour mener une attaque informatique massive la semaine dernière dans le monde, a menacé d'en révéler d'autres le mois prochain.

Dans un message posté tard mardi soir sur internet, le groupe indique dans un très mauvais anglais qu'il acceptera à partir de début juin des paiements en échange desquels les souscripteurs recevront chaque mois des informations sur des techniques de piratage et des vulnérabilités informatiques...[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 : *Cyberattaque: des hackers menacent de divulguer d'autres failles*

# WannaCrypt : une énorme épidémie de ransomwares perturbe les systèmes informatiques du monde entier



The image shows the main interface of the WannaCrypt ransomware. It features a dark red background with white and yellow text. At the top left is a padlock icon. The main text reads: "Oops, your files have been encrypted!". Below this, it explains that files are encrypted and provides instructions on how to recover them by paying in Bitcoin. A countdown timer shows "Time Left 02:23:34:22". At the bottom, there is a Bitcoin address field and buttons for "Check Payment" and "Decrypt".

**Oops, your files have been encrypted!**

**What Happened to My Computer?**  
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**  
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**  
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

**Payment will be raised on**  
5/15/2017 16:50:06  
Time Left  
02:23:34:22

**Your files will be lost on**  
5/19/2017 16:50:06  
Time Left  
06:23:34:22

[About bitcoin](#)  
[How to buy bitcoins?](#)  
[Contact Us](#)

**Send \$300 worth of bitcoin to this address:**  
115p7UMMngoj1pMvkpHjjeRdfJNXj6LrLn  
Copy

**Check Payment** **Decrypt**

WannaCrypt : une énorme épidémie de ransomwares perturbe les systèmes informatiques du monde entier

**Une nouvelle vague de ransomwares connus sous le nom de « WannaCrypt » (détectée par ESET sous Win32 / Filecoder.WannaCryptor.D) s'est répandue dans le monde entier. Ce ransomware a infecté des dizaines de milliers d'ordinateurs. Il se propage en exploitant une vulnérabilité Microsoft® Windows dans des ordinateurs non patchés.**

Touchant des centaines de milliers d'ordinateurs à travers le monde, la cyberattaque de vendredi est, de l'avis même d'Europol, « d'un niveau sans précédent ». A l'heure actuelle c'est plus de 75 000 victimes qui auraient été recensées dans le monde, parmi lesquelles le service public de santé britannique, le service de livraison FedEx, le ministère russe de l'Intérieur, des universités chinoises, l'opérateur télécom espagnol Telefonica, la compagnie ferroviaire allemande Deutsche Bahn ou encore Renault en France.

**ESET® détecte et bloque la menace WannaCryptor.D et ses variantes.** Le module de protection du réseau ESET bloque l'exploit au niveau du réseau. **ESET a alerté ses utilisateurs sur son site Internet. Toutes les instructions, étape par étape, sont renseignées pour qu'ils s'assurent d'être correctement protégés contre cette menace.**

Pour ESET, la sécurité du client a toujours été sa priorité. L'éditeur recommande aux utilisateurs de mettre à jour de manière proactive leurs systèmes d'exploitation, et de faire preuve de prudence lors de l'ouverture des pièces jointes. Dans ses solutions, ESET recommande d'activer LiveGrid.

**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