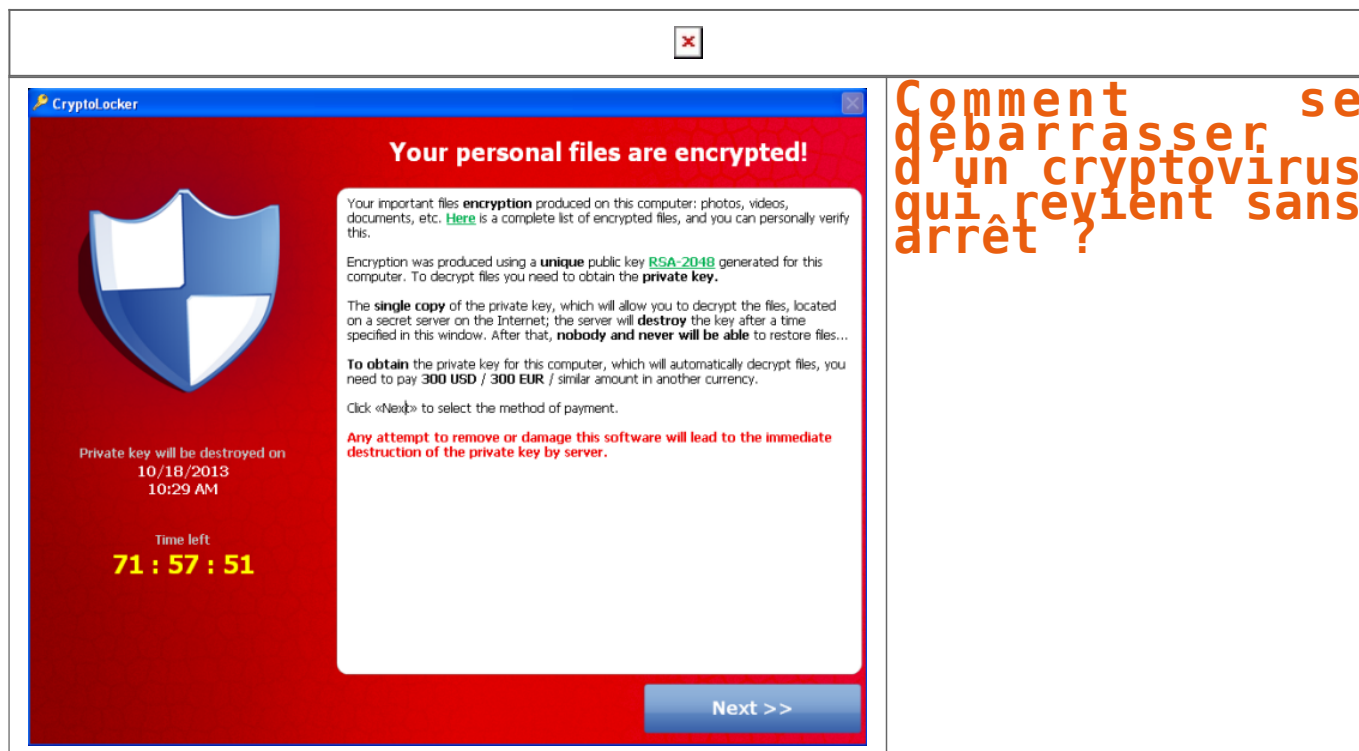


# Comment se débarrasser d'un cryptovirus qui revient sans arrêt ?



The image shows a screenshot of a Cryptolocker ransomware window. The window has a red background and a blue title bar with the text "Cryptolocker". On the left side, there is a blue shield icon with a white cross. Below the shield, it says "Private key will be destroyed on 10/18/2013 10:29 AM" and "Time left 71 : 57 : 51". In the center, there is a white text box with the following content:

**Your personal files are encrypted!**

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

**To obtain** the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

**Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.**

At the bottom right of the window, there is a blue button labeled "Next >>".

Overlaid on the right side of the window is the text "Comment se débarrasser d'un cryptovirus qui revient sans arrêt ?" in a large, orange, sans-serif font.

Vous vous êtes fait piéger par un Cryptovirus ? Après un bon nettoyage de l'ordinateur, vous avez réinstallé les fichiers perdus grâce à de précieuses sauvegardes. Cependant, quelques jours ou quelques semaines plus tard, vos fichiers sont à nouveau cryptés. Que faire ?

Que ça soit à la suite des nombreux défaçages de sites Internet (piratage du site Internet et changement de la page d'accueil) dont ont été victimes des dizaines de milliers de sites Internet en 2015 ou à la suite de vagues de virus cryptant la quasi totalité des données de votre ordinateur et vous demandant de payer une rançon pour continuer à les utiliser, nous avons été surpris par les mesures prises par le ou les informaticiens. En effet, à la suite d'échanges avec ces pomiers informatiques afin de vérifier les mesures prises à la suite de l'attaque informatique, nous avons eu, et leurs clients également, la désagréable surprise que leurs actions se restreignaient à nettoyer le ou les postes infectés et restaurer la dernière sauvegarde. En d'autres termes, excepté pour ceux profitant de cette situation pour constater que leurs systèmes de sauvegardes parfois lourdement facturés ne fonctionnaient pas ou ne sauvegardaient pas tout, la quasi totalité des techniciens contactés nous ont confirmé que le grand changement dans leurs procédures à la suite d'une telle attaque de pirate, consistait à renforcer la vérification des procédures de sauvegarde !!! Vous l'aurez compris, la conséquence évidente que si l'on ne soigne pas la cause du mal et qu'on ne fait qu'atténuer les effets, le mal reviendra. Sauf à ce que ça vous plaise de passer votre temps de restaurer des données à chaque nouvelle attaque, il est peut-être temps de changer quelque chose.

En cas d'attaque par ransomware (cryptovirus), nous vous recommandons de vous former ou d'utiliser un spécialiste pour suivre les étapes suivantes (l'ordre peut être adapté en fonction de vos priorités) :

1. Payer ? nous ne recommandons pas ça car non seulement vous favorisez le développement de ces actes en récompensant les cybercriminels, mais également rien ne vous assure que vous pourrez récupérer l'utilisation de vos fichiers et enfin, même si vous payez et que vous en avez pour votre argent, il est fort probable que le même pirate ou un autre vous piège à nouveau.
  2. Constatez et recueillez les preuves ;
3. Conservez les preuves soit pour une analyse ultérieure en vue de la recherche d'un antidote, soit pour une analyse approfondie de la technique utilisée par le pirate informatique, soit pour pouvoir porter plainte (si vous avez une assurance ou pour vous protéger si votre système informatique victime contient d'autres systèmes informatiques, ce qui vous rendrait responsable) ;
  4. Eventuellement, portez plainte ;
  5. Nettoyez votre système informatique de toutes traces du virus ;
6. Pour éviter qu'elle se reproduise, analysez avec précision l'attaque informatique afin de trouver la faille utilisée pour pénétrer votre système informatique en vue de sa réparation ;
  7. Restaurez les données pour pouvoir remettre en route son système informatique le plus rapidement possible ;
  8. Recherchez la faille ;
  9. Corrigez la faille ;
  10. Recherchez d'autres failles ;
11. Par prévention, corrigez d'autres failles et augmentez vos mesures de sécurité ;
12. Contactez éventuellement les autorités compétentes (Police, Gendarmerie, OCLCTIC, BETFI, votre CERT, le CERTA, PHAROS...) ;

Denis JACOPINI, Expert Informatique assermenté, est spécialisé en cybercriminalité et en protection des données personnelles pourra vous accompagner pour chacune de ces étapes.

[Contactez-nous](#)

Vous êtes une société d'informatique démunie devant une situation spécifique, il n'y a aucun inconvénient à vous faire aider par un spécialiste en cybercriminalité. Nous pouvons également vous accompagner.

**Remarque 1**

Certaines de ces étapes peuvent être longues et nécessiteront un accès à distance de votre installation.

[Régissez à cet article](#)

## 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
  - ALL RGPD
  - LA FONCTION DE DPO

### RECHERCHE DE PREUVES (outils Gendarmerie/Police)

- ORDINATEURS (Photos / E-mails / Fichiers)
- TELEPHONES (récupération de Photos / SMS)
- SYSTEMES NUMERIQUES

### EXPERTISES & AUDITS (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- SECURITE INFORMATIQUE
- SYSTEMES DE VOTES ELECTRONIQUES

### Besoins 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 DORTTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisée en « Sécurité » Cybercriminalité et en RGPD (Protection des Données & Conformité).

Accompagnement à la mise en place de DPO ;

Cartographie et sensibilisation à la sécurité des données ;

Audit Sécurité (ISO 27005) ;

Expertises techniques et judiciaires ;

Enquêtes, témoignages, déclarations, e-mails, contenus, documents de données ;

Domaines de spécialité de votre électronique ;

**Le Net Expert**

**INFORMATIQUE**

Consultant en Informatique

[Contactez-nous](#)

Vous manipulez ou stockez des données (coordonnées postales, informations financières, ou médicales et bien d'autres tout sans limites) au contact de vos clients, fournisseurs, prospects... En tant que responsable de traitement, vous êtes tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques prévus par le traitement, pour préserver la sécurité des données (Article 32 du RGPD).

VOUS DEVEZ DONC :

Mettre en conformité votre établissement en mettant en conformité l'ensemble de vos traitements de données personnelles notamment en identifiant, retravaillant, archivant ou plus généralement agissant entre autres sur :

- La durée de conservation de vos données
- Les moyens de collecte
- Le respect de « Privacy by Design »
- Le principe d'« Accessibilité »

- Une analyse d'impact.

Nous pouvons vous accompagner dans votre démarche mise en conformité en accompagnant une personne dans votre établissement que nous ferons travailler en complément pour une satisfaction de votre établissement.

Besoin d'informations complémentaires ?

[Contactez-nous](#)

Denis JACOPINI

Formateur n°93 84 03041 84