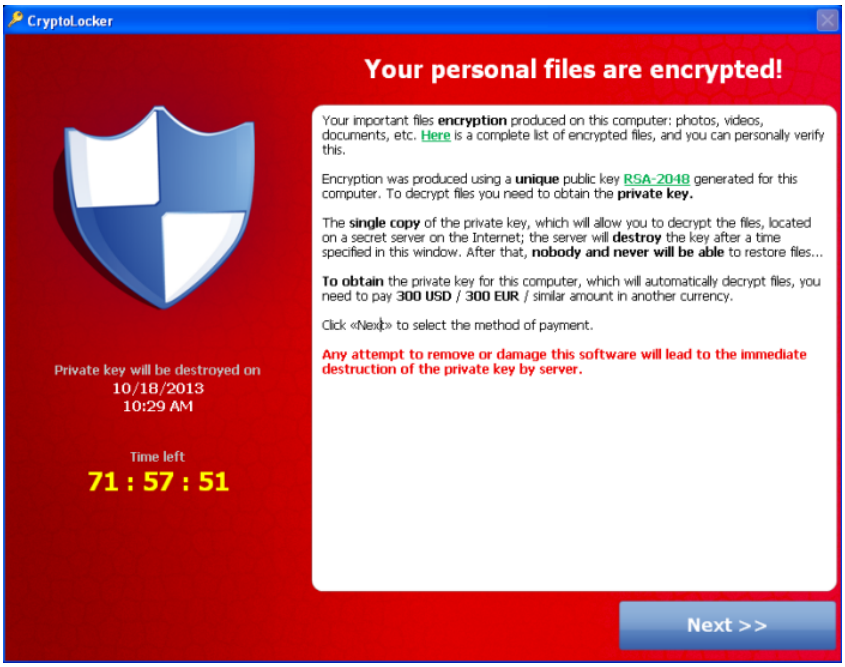
Comment se débarrasser d’un cryptovirus qui revient sans arrêt ?



Comment se débarrasser d’un cryptovirus qui revient sans arrêt ?

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 pompiers 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 fonctionnait pas ou ne sauvegardait pas tout, la quasi totalité des techniciens contactés nous ont confirmé que le grand changement dans leurs procédure 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 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 contamine d'autres systèmes informatique , ce qui vous rendraient responsable) ;
4. Éventuellement, 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 :
Certaines de ces étapes peuvent être longues et nécessiteront un accès à distance de votre installation.

Réagissez 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**
  - **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).