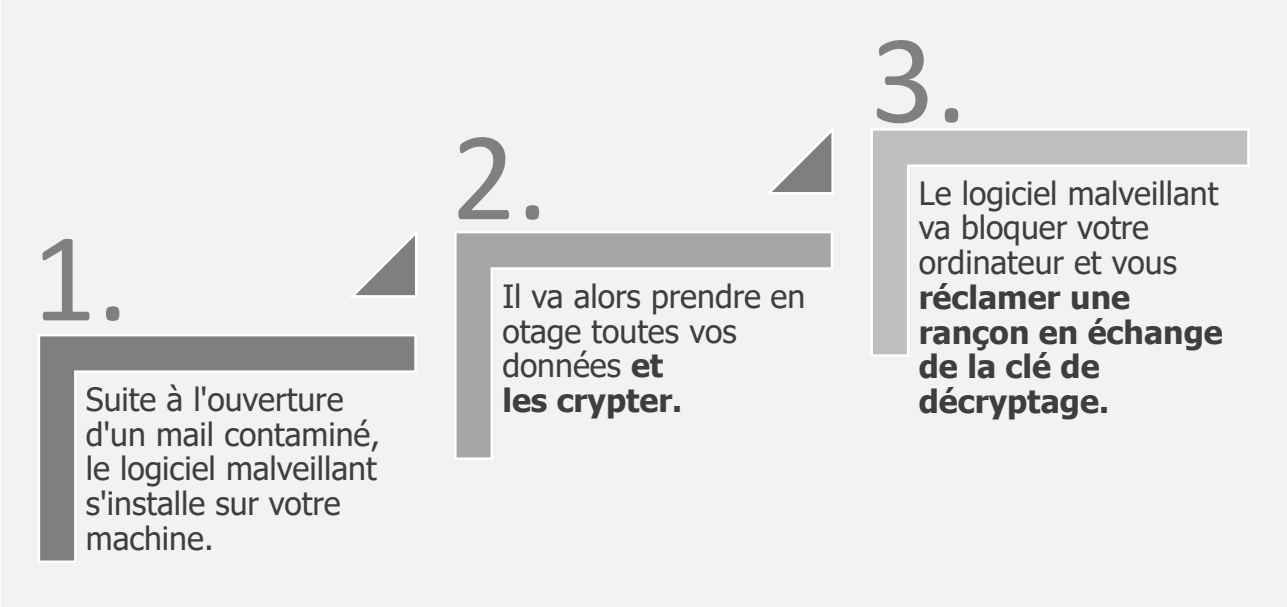
#1 Livre Blanc

Cryptolocker, comment répondre à la menace croissante des ransomware ?

Le CryptoLocker, dit « rançongiciel » (ransomware), est un logiciel malveillant qui vous empêche d'utiliser vos fichiers en les cryptant, puis vous extorque de l'argent en échange d'une promesse de les déverrouiller. Les montants des rançons oscillent entre 100 et des milliers de dollars. La rançon peut dans certains cas être acquittée en bitcoins[1].

Ce virus se propage **par courrier électronique à l'ouverture d'une pièce jointe** très souvent au format .doc, .excel ou d'un fichier zippé (.zip). Au premier clic sur cette pièce jointe l'ensemble des données de l'ordinateur et des lecteurs réseaux connectés sont cryptés. **L'utilisateur et/ou la société sont alors « pris en otages et rançonnés ».**

Méthode de l'attaque



[1] Monnaie virtuelle

Comment se protéger d'un Cryptolocker ?

Comme dans la majorité des cas, les virus se propagent par mail. C'est également le cas avec le Virus Cryptolocker. Il faut prêter attention à chaque détail avant d'ouvrir une pièce jointe d'un email.

Voici quelques conseils de prévention :

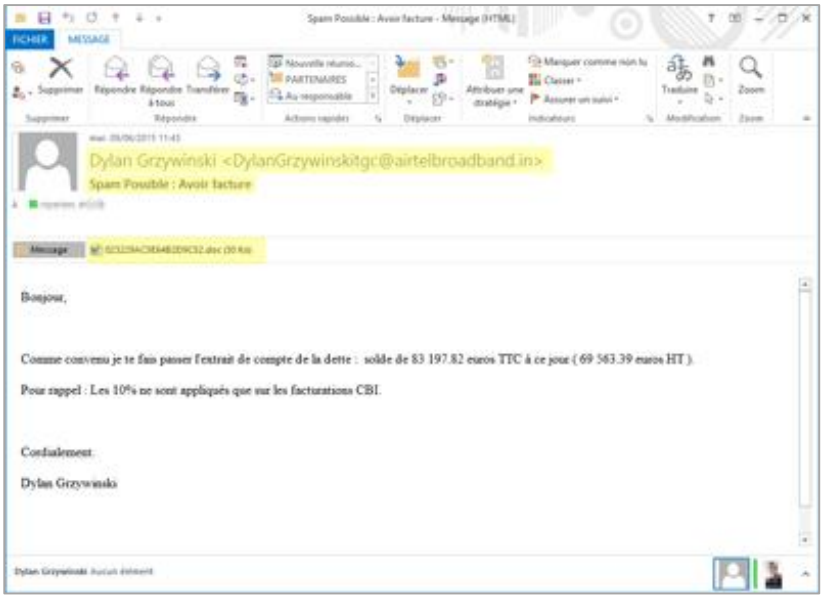
- **Conseil N°1 : Etudiez les caractéristiques de vos messages avant de les ouvrir**
  Les e-mails avec pièces jointes inférieures à 70 ko, envoyés par des inconnus et rédigés en anglais sont très probablement porteurs de virus. Attention aux fichiers à **doubles extensions**, par exemple, « ma-photo.jpg.pif » ou « lettre.doc.vbs », *etc.* Seule la dernière extension compte. Les fichiers .pif, .vbs, .exe, .com et .cpl sont généralement des virus.

- **Conseil N°2 : Ne prenez pas ce qui est écrit pour argent comptant**
  Prenez le temps d'étudier les caractéristiques de votre message (mail de l'expéditeur, langue, orthographe, taille, type et nom du fichier attaché) avant d'ouvrir une pièce jointe. Dans le doute sur l'origine et le contenu du message, **ne jamais ouvrir la pièce jointe** et informer votre service informatique.

- **Conseil N°3 : Sauvegardez vos données de manière régulière**
  Faites des sauvegardes régulières de vos documents sensibles.
  Votre service informatique ne doit pas négliger la mise en place de solutions de sauvegarde sur bandes, sur disques et/ou externalisées pour garantir un temps de rétablissement (RTO) optimal en cas d'infection.

- **Conseil N°4 : Protégez-vous**
  Utilisez un anti-virus et un anti-spam à jour et vérifiez quotidiennement la disponibilité des mises à jour.

Exemple d'un mail avec une pièce jointe Cryptolocker :



Que faire si vous êtes contaminé par un Cryptolocker ?

NE PAYEZ PAS.

Vous n'avez aucune garantie que vos fichiers seront décryptés. Les clés de décryptages sont très souvent inutilisables. Vous aurez perdu vos données et votre argent.

Le chiffrement prend du temps, si vous vous rendez compte que Cryptolocker est à l'œuvre sur votre machine :

1. **Déconnectez les appareils** des réseaux partagés, avec ou sans fil
2. **Dépêchez-vous de stopper l'attaque en débranchant le câble Ethernet ou la connexion Wifi** pour ne pas propager le cryptage à l'ensemble des documents de l'entreprise
3. **Eteignez votre poste** et prévenez le service informatique de votre société

Si vous agissez vite, vous aurez aussi peut-être la chance que vos fichiers ne soient pas tous chiffrés. Seule solution viable et efficace, restaurer ses données grâce à des sauvegardes des systèmes impactés.

En résumé

L'utilisateur doit :

- Etre sensibilisé aux risques : perte de ses données et celles de l'entreprise,
- **Analyser les caractéristiques de chaque email reçu** (nom, adresse mail, sujet),
- Analyser le contenu d'un email avant d'ouvrir une pièce jointe,
- Mettre à jour les logiciels et applications directement sur les sites officiels,
- Maintenir l'antivirus toujours actif et à jour,
- Utiliser des anti-spam et des pare-feu pour diminuer les risques.

J'ai besoin d'aide