

# Infectée par un cryptolocker, la police du Massachusetts paie 500\$ de rançon | Le Net Expert Informatique



**Infectée par un cryptolocker, la police du Massachusetts paie 500\$ de rançon**

**La police de la ville de Tewksbury, dans le Massachusetts, victime d'un cryptolocker, a du régler 500\$ pour déchiffrer les fichiers conservés sur un serveur afin de remettre ses équipes au travail.**

Un Département de police du Massachusetts, celui de la ville de Tewksbury, a du verser 500 \$ à un cyberpirate pour débloquer les fichiers chiffrés avec un cryptolocker, le ransomware qui verrouille les disques durs jusqu'à ce que les propriétaires paient une rançon. Après plusieurs jours d'essais infructueux, les services informatiques de la police de Tewksbury ont réalisé qu'ils ne pouvaient pas casser le chiffrement et payé la rançon pour obtenir la clef privée permettant d'accéder aux données.

« Ils ont rendu inopérant le logiciel que nous utilisons pour assurer le fonctionnement du Département de la police », a déclaré le chef de la police, Timothy Sheehan, au journal Tewksbury Town Crier. L'incident est survenu à la fin de l'année dernière, l'infection a démarré le 7 décembre sur un poste de travail.

#### **Une attaque très ciblée**

Les attaquants ont exploré le réseau jusqu'à corrompre le serveur principal du Département. Les services de Police sauvegardent leurs fichiers sur un disque dur externe qui a également été touché par le ransomware, de sorte qu'ils avaient le choix de payer 500 \$ ou de perdre toutes les données.

La police de l'État et le FBI se sont penchés sur cette affaire, tout comme Delphi Technology Solutions et Stroz Friedberg, des sociétés spécialisées dans la police scientifique. Aucune des deux n'a réussi à casser le cryptage de sorte que le Département a payé, indique le journal local. Stroz Friedberg a converti les 500 \$ de la rançon en bitcoins avant de l'envoyer de la part du Département de police.

#### **Payer ou pas**

Les applications affectées concernaient la répartition des tâches assignées aux différents agents, la gestion des documents, la main courante avec les arrestations et la conservation des appels au commissariat. La même mésaventure s'est déjà produite en 2013 dans un autre service de police à Swansea, toujours dans le Massachusetts ; 750\$ avaient alors été réglés pour débloquer le système.

De nombreux experts estiment que les victimes auraient du refuser de payer, surtout s'ils s'agit des forces de l'ordre, mais après avoir examiné l'alternative, c'est-à-dire ne jamais revoir ses données, de nombreuses entreprises préfèrent payer afin de recommencer à travailler.

---

Expert Informatique assermenté 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.lemondeinformatique.fr/actualites/lire-infectee-par-un-cryptolocker-la-police-du-massachusetts-paie-500-de-rancon-60783.html>  
Par Serge Leblal