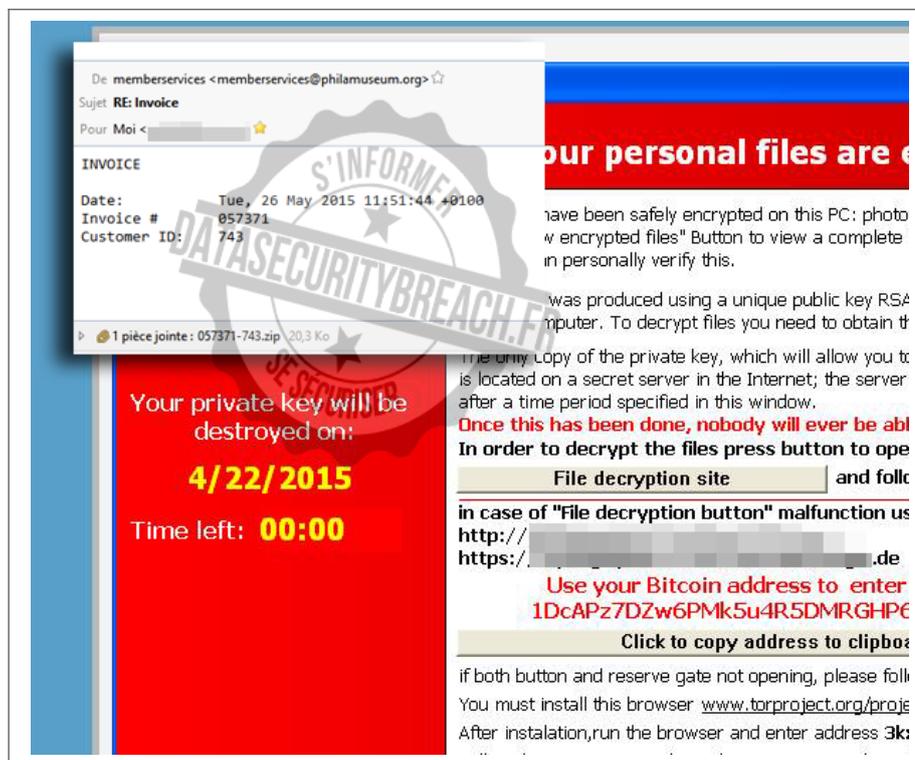


# Mise à disposition de l'outil de déchiffrement contre le ransomware Polyglot



The screenshot shows an email interface with the following details:

- From:** memberservices <memberservices@philamuseum.org>
- Subject:** RE: Invoice
- To:** Moi <[redacted]>
- INVOICE**
- Date:** Tue, 26 May 2015 11:51:44 +0100
- Invoice #:** 057371
- Customer ID:** 743
- Attachment:** 1 pièce jointe : 057371-743.zip (20.3 Ko)

The main body of the email contains the following text:

**our personal files are e**

have been safely encrypted on this PC: photo  
w encrypted files" Button to view a complete  
in personally verify this.

was produced using a unique public key RSA  
mputer. To decrypt files you need to obtain th

The only copy of the private key, which will allow you to  
is located on a secret server in the Internet; the server  
after a time period specified in this window.

**Once this has been done, nobody will ever be abl**

**In order to decrypt the files press button to ope**

**File decryption site** and folk

in case of "File decryption button" malfunction us  
http://  
https://[redacted].de

**Use your Bitcoin address to enter**  
**1DcAPz7DZw6PMk5u4R5DMRGHP6**

**Click to copy address to clipbo**

if both button and reserve gate not opening, please foll  
You must install this browser [www.torproject.org/proje](http://www.torproject.org/proje)  
After instalation,run the browser and enter address **3k:**

**Watermark:** S'INFORMER, DATA SECURITY BREACH, DE SECURITE

Mise à disposition de l'outil de déchiffrement contre le ransomware Polyglot

**Les victimes du ransomware Polyglot, aussi connu sous le nom MarsJoke, peuvent maintenant récupérer leurs fichiers grâce à l'outil de déchiffrement développé par Kaspersky Lab.**

Comment fonctionne Polyglot ? Il se propage via des emails de spam qui contiennent une pièce jointe malicieuse cachée dans une archive RAR. Durant le processus de chiffrement, il ne change pas le nom des fichiers infectés mais en bloque l'accès. Une fois le processus de chiffrement terminé, le wallpaper de bureau de la victime est remplacé par la demande de rançon. Les fraudeurs demandent que l'argent leur soit remis en bitcoins et si le paiement n'est pas fait dans les temps, le Trojan se détruit en laissant tous les fichiers chiffrés.

### **Lien avec CTB-Locker ?**

Le fonctionnement et le design de ce nouveau ransomware sont proches de ceux de CTB-Locker, un autre ransomware découvert en 2014 qui compte de nombreuses victimes à travers le monde. Mais après analyse, les experts de Kaspersky Lab n'ont trouvé aucune similarité dans le code. En revanche, contrairement à CTB-Locker, le générateur de clés de chiffrement utilisé par Polyglot est faible. Les créateurs de Polyglot semblaient penser qu'en imitant CTB-Locker, ils pourraient piéger les utilisateurs en leur faisant croire qu'ils étaient victimes d'un grave malware, ne leur laissant d'autre option que de payer...[Téléchargez l'outil]

Article de Data Security Breach

---

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



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

Original de l'article mis en page : Outil de déchiffrement contre le ransomware Polyglot – Data Security Breach  
Data Security Breach