



CYBERATTQUES 2015-2016

Les arnaques au président,
Les rançongiciels



Major Fabrice Crasnier
(Commandant de la Division Analyse Criminelle et Cybercriminalité)
Forensic IT / PhD Student



CYBERATTQUES



L'arnaque au président ou escroquerie aux faux ordres de virement international (FOVI)

Fraude aux Faux Ordres de Virement #FOVI



1
L'escroc collecte des informations pour connaître l'entreprise et ses dirigeants (réseaux sociaux, organigramme)



2
Se faisant passer pour le dirigeant de l'entreprise, l'escroc prétexte une opération financière urgente et confidentielle



3
Sous la pression ou en confiance, l'entreprise exécute la transaction



4
L'escroc transfère l'argent vers des comptes basés à l'étranger

CYBERATTAQUES



L'arnaque au président ou escroquerie aux faux ordres de virement international (FOVI)

Les escrocs se renouvellent régulièrement.

- L'escroquerie « *au faux président* »
- L'escroquerie « *au faux fournisseurs* »
- L'escroquerie « *au changement de Relevé d'Identité Bancaire* »
- L'escroquerie « *au virement SEPA, à l'informatique* »

5 ans d'existence
Plusieurs centaines de millions d'euros

CYBERATTAQUES



L'arnaque au président ou escroquerie aux faux ordres de virement international (FOVI)

Que faire en cas d'attaque ?

- Demander immédiatement à la banque le retour des fonds **dans les 24 H.**
- Déposer une plainte auprès des services de police et de gendarmerie, en apportant un maximum d'éléments (mail, téléphone, etc...). **Dans les 48 H maximum**

Un dépôt de plainte **rapide** permet d'optimiser les chances de récupérer les fonds escroqués.



CYBERATTAQUES

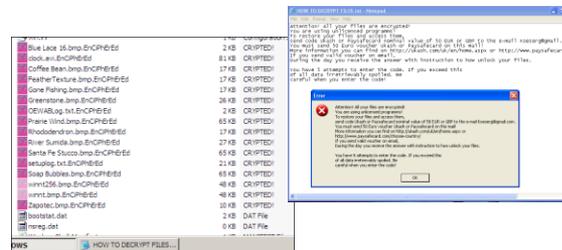


Les Rançongiciels (Ransomwares)

Janvier 2011 – 2016++



Les rançongiciels policiers



Ransomware Cerber WebExploit.

Mars/Avril/Mai 2016 :
Nouveau Ransomware
CryptXXX provenant de
la Team Reveton



En 2014 et 2015,
CTB-Locker, TeslaCrypt
et Cryptowall



Petya Ransomware,
moins actif, un
Ransomware MBR

Les Rançongiciels (Ransomwares)

« **Un rançongiciel** est un programme malveillant dont l'objectif est de chiffrer partiellement ou entièrement les données sur le système cible.

En fonction des privilèges d'exécution et des mesures de sécurité du poste, le programme malveillant chiffre les données de la session de l'utilisateur, les fichiers partagés via les lecteurs réseau, voire les données du système.



L'objectif est de proposer à la victime de récupérer ses données en l'échange du paiement d'une rançon. »

<http://cert.ssi.gouv.fr/site/CERTFR-2016-ACT-016/>

(en date du 18 Avril 2016 – date de consultation : 17/05/2016)

CYBERATTQUES



Les Rançongiciels (Ransomwares)

Janvier 2011 – 2016++

New variants of ransomware known as **CryptoLocker**, **CryptoDefense** and **CryptoWall** are spreading via spam emails, drive-by downloads, or by malware already on your computer. Once you're infected, **crypto-ransomware** hijacks all your files, locks them up with unbreakable encryption, and demands a ransom of \$300-\$500 in bitcoins to unscramble them.

5 STAGES OF CRYPTO-RANSOMWARE

1 INSTALLATION

After a victim's computer is infected, the crypto-ransomware installs itself, and sets keys in the Windows Registry to start automatically every time your computer boots up.



2 CONTACTING HEADQUARTERS

Before crypto-ransomware can attack you, it contacts a server operated by the criminal gang that owns it.



3 HANDSHAKE AND KEYS

The ransomware client and server identify each other through a carefully arranged "handshake," and the server generates two cryptographic keys. One key is kept on your computer, the second key is stored securely on the criminals' server.



4 ENCRYPTION

With the cryptographic keys established, the ransomware on your computer starts encrypting every file it finds with any of dozens of common file extensions, from Microsoft Office documents to .JPG images and more.

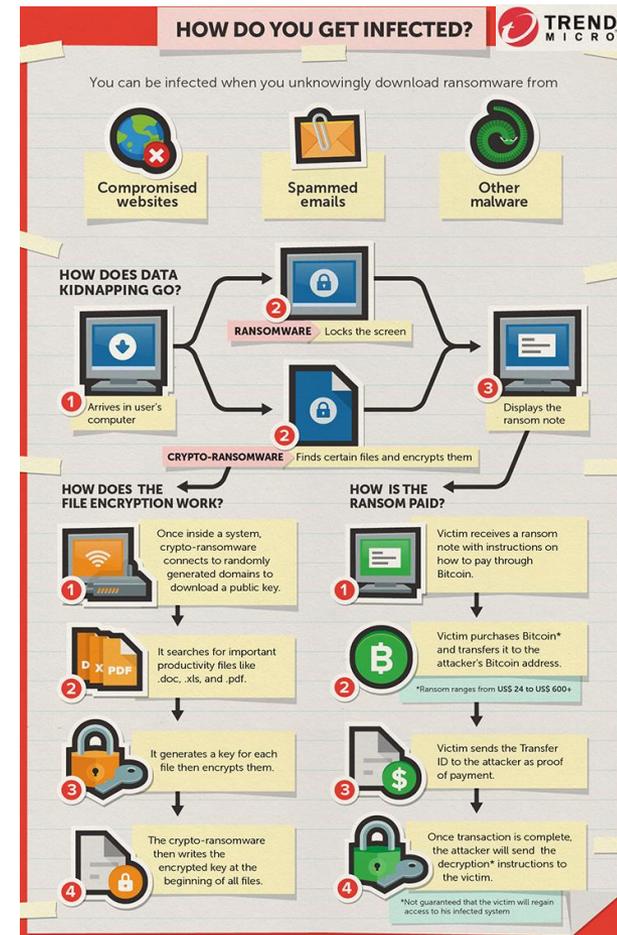


5 EXTORTION

The ransomware displays a screen giving you a time limit to pay up before the criminals destroy the key to decrypt your files. The typical price, \$300 to \$500, must be paid in untraceable bitcoins or other electronic payments.



SOPHOS
Security made simple.



CYBERATTAQUES



Les Ransomwares (Cryptolocker)

Janvier 2013 – 2016++

Trojan Banker Dridex

TeslaCrypt Ransomware

(TeslaCrack)

Jigsaw



Locky Ransomware



52 ransomwares différents

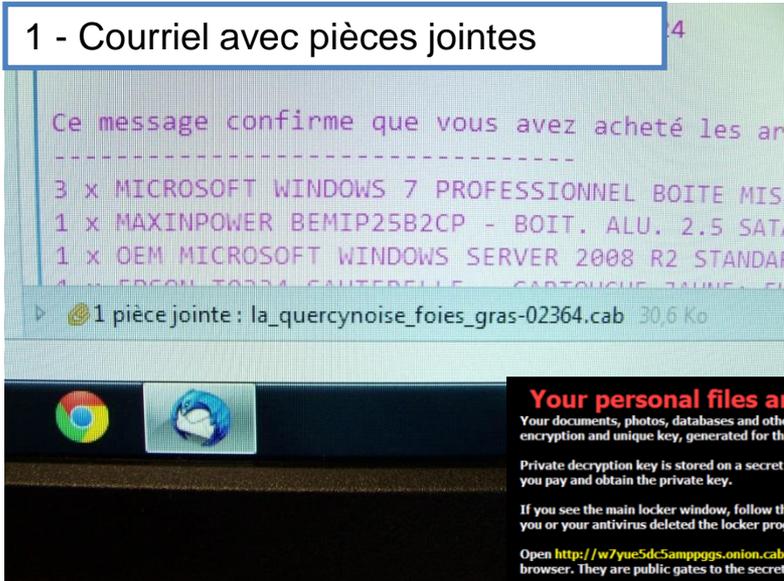
CYBERATTAQUES



Les Ransomwares (Cryptolocker)

Janvier 2015

1 - Courriel avec pièces jointes



Your personal files are encrypted by CTB-Locker

Your documents, photos, databases and other important files have been encrypted with strong encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

If you see the main locker window, follow the instructions on the locker. Otherwise, it's possible that your antivirus deleted the locker program. Now you have the last chance to decrypt your files.

Open <http://w7yue5dc5amppggs.onion.cab> or <http://w7yue5dc5amppggs.tor2web.org> in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:

1. Download Tor Browser from <http://torproject.org/>
2. In the Tor Browser open the <http://w7yue5dc5amppggs.onion/>
Note that this server is available via Tor Browser only. Retry in 1 hour if site is not reachable.

Write in the following public key in the input form on server. Avoid missprints.
AZRASU2-2A6ZXGH-GFY3UNG-DS7FPHJ-NXMPFYZ-SU4BCFR-QMM7DWL-5LE7J4M
CFJR47M-3YW6BCM-EEPHMK2-FLAVNNG-427Y5AU-FNXAK6T-YAXPXI3-T6RPHQR
DB2CD6T-5L2XSDP-EIC7AAY-KKJA3YH-KEA2SYW-RGQRNZZ-655X4TA-UIRV7XJ

2 – demande de rançon

3 – Lieu de paiement



CYBERATTQUES



Les Ransomwares (Cryptolocker)

Janvier 2016

Locky Decryptor

twbers4hmi6dx65f.onion/F39397E567D45A86

Rechercher

Langues: Français

Locky Decryptor™

Nous présentons un logiciel special - Locky Decryptor™ - permettant de déchiffrer et gérer tous vos fichiers codifiés.

Comment acheter Locky Decryptor™?

- 1 Vous avez la possibilité de payer en bitcoins, on peut les obtenir par des voies différentes.
- 2 Il vous faut enregistrer un portefeuille:
[Le plus simple portefeuille](#) ou [autres moyens de création de portefeuille.](#)
- 3 Malgré le fait qu'il n'est pas si simple d'obtenir des bitcoins, leur achat devient moins compliqué de jour en jour.

Nos recommandations:
[localbitcoins.com \(WU\)](#) Achat des bitcoins avec WesternUnion.
[coincafe.com](#) Un service rapide et simple.
Modes de paiement: WesternUnion, BankofAmerica, obtention de l'argent en espèce par FedEx, Moneygram, virement. A New-York: distributeur des bitcoins, personnellement.
[localbitcoins.com](#) Ce service vous permet de trouver des gens dans votre agglomération, qui sont prêts à vous vendre des bitcoins directement.
[cex.io](#) Achat des bitcoins à l'aide de VISA/MASTERCARDou par virement bancaire.
[btcdirect.eu](#) Le meilleur site pour l'Europe.
[bitquick.co](#) Achat instantané des bitcoins en numéraire.
[howtobuybitcoins.info](#) Direction internationale d'échange des bitcoins.
[cashintocoins.com](#) Achat des bitcoins en numéraire.
[coinjar.com](#) Sur le site CoinJaron peut acheter des bitcoins directement.
[anxpro.com](#)

4 Envoyez 4.00 BTC sur la bitcoin adresse:

1MfTa1xbah44TdCzZir4LuDjofAgLe1He6

Remarque: pour que la transaction soit confirmée le paiement peut être en état de traitement pendant 30 minutes et plus, patientez...

- 5 Mettez à jour la page et téléchargez le déchiffreur.
Après avoir reçu une confirmation de transaction en bitcoins, vous allez être redirigé sur une page pour le téléchargement du déchiffreur.

Langues: Français

- Bългарски
- Català
- Čeština
- Dansk
- Ελληνικά
- English
- Español
- Français**
- Hrvatski
- Magyar
- Italiano
- 한국어
- Nederlands
- Norsk bokmål
- Polski
- Português
- Slovenčina
- Српски
- Svenska
- Türkçe

Recommandations

L'arnaque au président

Les Ransomwares (Cryptolocker)



L'arnaque au président ou escroquerie aux faux ordres de virement international (FOVI)

Quelques règles simples

Pour s'en prémunir, les entreprises peuvent mettre en place un ensemble de mesures simples de sécurité pour décourager les escrocs.

- **Rappeler à l'ensemble des collaborateurs** la nécessité d'avoir un usage prudent des réseaux sociaux privés et professionnels. Les alerter sur l'importance de ne pas y divulguer d'informations concernant le fonctionnement de l'entreprise.
- Sensibiliser **régulièrement l'ensemble des employés des services comptables, trésorerie, secrétariats, standards**, de ce type d'escroquerie. Prendre l'habitude d'en informer systématiquement les **remplaçants** sur ces postes.
- **Instaurer des procédures de vérifications** et de signatures multiples pour les paiements internationaux et **saisir soi-même l'adresse habituelle du donneur d'ordre**.
- Accentuer la vigilance sur les **périodes de congés scolaires**, les **jours fériés** et les **jours de paiement des loyers**.

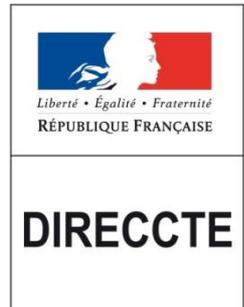
CYBERATTQUES



L'arnaque au président ou escroquerie aux faux ordres de virement international (FOVI)

Prévention à la cybersécurité:

- Direction régionale des entreprises, de la concurrence, de la consommation, du travail et de l'emploi (**DIRECCTE**)
- Direction générale de la Sécurité intérieure (**DGSI**)
- **Gendarmerie Nationale** (Intelligence Economique)
- Direction de la Protection et de la Sécurité de la Défense (**DPSD**)
- Le pôle de compétitivité **Aerospace valley**
- **Réserve Citoyenne Cyberdéfense (RCC)**



Les Ransomwares (Cryptolocker)

Janvier 2013 – 2016++

Que faire en cas de compromission ?

1. **Positionner les permissions des dossiers partagés** en LECTURE SEULE afin d'empêcher le chiffrement des fichiers sur ceux-ci ,
2. **Bloquer la poursuite du chiffrement** des documents en **déconnectant du réseau les postes identifiés**,
3. **Prendre contact immédiatement avec la chaîne de sécurité informatique de votre entité**, afin de signaler l'incident (service informatique, RSSI, DSI)
4. **Déposer plainte** : réunir toutes les traces et indices qui pourraient servir comme éléments de preuve :
 - *copies physiques des disques durs (ou VM) des postes compromis (conserver les dates de modifications des fichiers)*
 - *copies des journaux d'événements disponibles sur tout équipement réseau qui auraient pu permettre la communication des codes malveillants (proxy, pare-feu, etc.), en conservant leur format d'origine et concernant la période estimée de compromission.*
5. **Bloquer les échanges** avec les serveurs mandataires : l'accès aux domaines, **IP ou URLs identifiés dans le message malveillant**, afin de prévenir toute nouvelle compromission sur le même site.

Les Ransomwares (Cryptolocker)

Janvier 2013 – 2016++

Que faire en cas de compromission ?

6. **Rechercher et supprimer les copies des pourriels identifiés** non encore distribuées dans les boîtes de messagerie des utilisateurs.
7. **Mettre en œuvre une politique de filtrage des passerelles de messagerie** (filtrage CAB, JS, EXE, etc.)
8. **Installer un antivirus sur les postes clients.** Un antivirus adapté aux passerelles de messagerie peut permettre d'éliminer en amont les pourriels détectés malveillants.
9. **Maintenir à jour les composants systèmes et applicatifs** : la mise à jour régulière des systèmes d'exploitation et des applications présentes, demeure une action fondamentale, sans oublier les navigateurs, briques Java, Adobe Flash Player, suites bureautiques, etc. A noter que les versions obsolètes doivent être remplacées en priorité
10. **Ne pas activer les macros pour les documents Office.** L'auto-exécution de ces macros est désactivée par défaut. Même si l'ouverture d'un document vous incite à réactiver celles-ci, ne le faites pas, surtout lorsque l'origine est douteuse. Lorsque ces macros sont nécessaires pour certains documents, le centre de sécurité Microsoft Office permet d'activer celles-ci uniquement pour les documents chargés depuis une liste d'emplacements spécifiés

Les Ransomwares (Cryptolocker)

Janvier 2013 – 2016++

Que faire en cas de compromission ?

- 11. Réinstaller le poste après éradication** : dernières mises à jour (OS et applicatives) et restauration d'une sauvegarde réputée saine des données de l'utilisateur. Supprimer la copie serveur des profils itinérants afin de prévenir l'éventuelle répétition d'exécution des codes malveillants par ce biais.
- 12. Ne pas payer la rançon** : le paiement ne garantit pas le déchiffrement des données et compromettra le moyen de paiement utilisé (notamment carte bancaire).
- 13. Conserver les fichiers au cas où**, dans le futur, un moyen de recouvrement des données originales serait découvert
- 14. Vérifier les autorisations d'accès aux ressources partagées** (ACL sur le partage et sur le système de fichiers) : notamment, les ressources accessibles en écriture doivent être limitées aux seuls utilisateurs qui en ont le besoin fonctionnel
- 15. Appliquer le principe du moindre privilège**, en attribuant aux différents comptes les seuls privilèges qui leur sont strictement nécessaires dans l'exécution de leurs tâches

Les Ransomwares (Cryptolocker)

Janvier 2013 – 2016++

Que faire en cas de compromission ?

16. **Implémenter les stratégies de restrictions logicielles** : SRP pour Windows XP et AppLocker pour Windows Vista et supérieur, ces stratégies visent à empêcher l'exécution de code à partir d'une liste noire de répertoires prédéfinis
17. **Sauvegarder les systèmes ainsi que les données**. La politique de sauvegarde doit également être adaptée, de telle sorte que les sauvegardes antérieures ne soient pas simplement écrasées, la sauvegarde la plus récente pouvant contenir une version chiffrée des données
18. **Éprouver le processus de restauration** : dans le cas où la prestation de sauvegarde/restauration est externalisée, il convient de s'assurer que les points de contact sont clairement identifiés ; des tests réguliers doivent être menés afin de valider l'intégrité des données restaurées;
19. **Bloquer les adresses utilisées par le code malveillant**

Les Ransomwares (Cryptolocker)

Janvier 2013 – 2016++

Que faire en cas de compromission ?

- 20. Sensibilisation des utilisateurs face aux risques associés aux messages électroniques.** Il convient en effet de ne pas cliquer sans vérification sur les liens ou ouvrir les pièces jointes présentes ; une attention toute particulière devant être apportée aux messages de provenance inconnue, l'apparence inhabituelle ou frauduleuse. L'expérience montre également qu'un exemple de courriels issus d'une campagne en cours est plus efficace qu'une sensibilisation « générique »



CYBERATTQUES

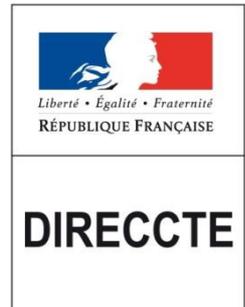


Les Ransomwares (Cryptolocker)

Janvier 2013 – 2016++

Prévention à la cybersécurité:

- Direction régionale des entreprises, de la concurrence, de la consommation, du travail et de l'emploi (**DIRECCTE**)
- Direction générale de la Sécurité intérieure (**DGSI**)
- **Gendarmerie Nationale** (Intelligence Economique)
- Direction de la Protection et de la Sécurité de la Défense (**DPSD**)
- Le pôle de compétitivité **Aerospace valley**
- **Réserve Citoyenne Cyberdéfense (RCC)**



Le réseau **CYBERGEND** fait face à la cyber criminalité



VOLET JUDICIAIRE

La gendarmerie s'adapte en permanence à l'évolution de la menace grâce au réseau **CYBERGEND en Région Midi-Pyrénées**

Echelon régional
(3)

N-Tech

- SAJ (1)** - Assistanes, Formations, Interventions et Audits de procédures
- SR (2)** - Direction d'enquêtes en cybercriminalité

Echelon Départemental
(8)

BR – BDRIJ – CIC – Assistanes aux unités

Echelon Élémentaire
(200)

Correspondants
N-Tech

BT – Assistanes aux enquêteurs



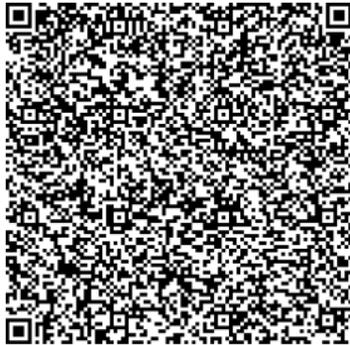


Gendarmerie Nationale

Section d'appui judiciaire de de la région Midi-Pyrénées
Division analyse criminelle et investigations spécialisées.



Merci de votre attention



Major Fabrice CRASNIER

*Commandant de la division analyse criminelle
et investigations spécialisées*

*Directeur d'enquêteur judiciaire spécialisé
en technologie numérique et délinquance financière.*

*Pilote du relais Cyberdéfense de la réserve citoyenne de la
région Midi-Pyrénées*

Chef de projet

Ingénieur en informatique en conception et développement

Doctorant en informatique

Ecole doctorale de Mathématiques Informatique

Télécommunications de Toulouse EDMITT.

(Laboratoire IRIT – Equipe SMAC)

Tel : 06.24.49.39.20

Courriel : fabrice.crasnier@gendarmerie.interieur.gouv.fr



Institut de Recherche en Informatique de Toulouse