CYBERATTAQUES 2015-2016

Les arnaques au président,
Les rançongiciels

UNIVERSITÉ TOULOUSE III PAUL SABATIER — Université de Toulouse

Major Fabrice **Crasnier**
(Commandant de la Division Analyse Criminelle et Cybercriminalité)
Forensic IT / PhD Student
IRIT CNRS - INPT - UPS - UT1 - UT2J

CYBERATTAQUES

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

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**

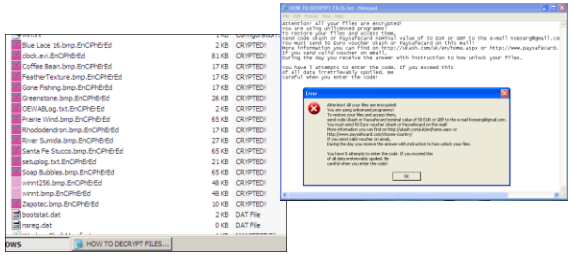
Un dépôt de plainte **rapide** permet d'optimiser les chances de récupérer les fonds escroqués.

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

https://stopransomware.fr/

CYBERATTAQUES

Les Rançongiciels (Ransomwares)

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

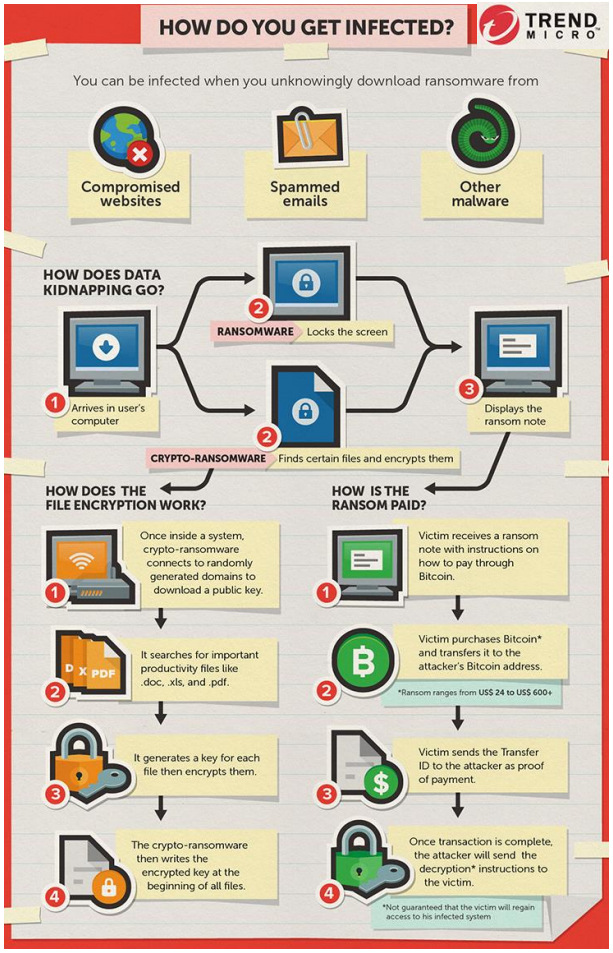
En fonction des privilèges d'exécution et des mesures de sécurité du poste, le programme malveillant chiffre les données de la session de l'utilisateur, les fichiers partagés via les lecteurs réseau, voire les données du système.

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

CYBERATTAQUES

Les Rançongiciels (Ransomwares)

Janvier 2011 – 2016++



CYBERATTAQUES

Les Ransomwares (Cryptolocker)

Janvier 2013 – 2016++

Trojan Banker Dridex

TeslaCrypt Ransomware

(TeslaCrack)

Jigsaw

Locky Ransomware

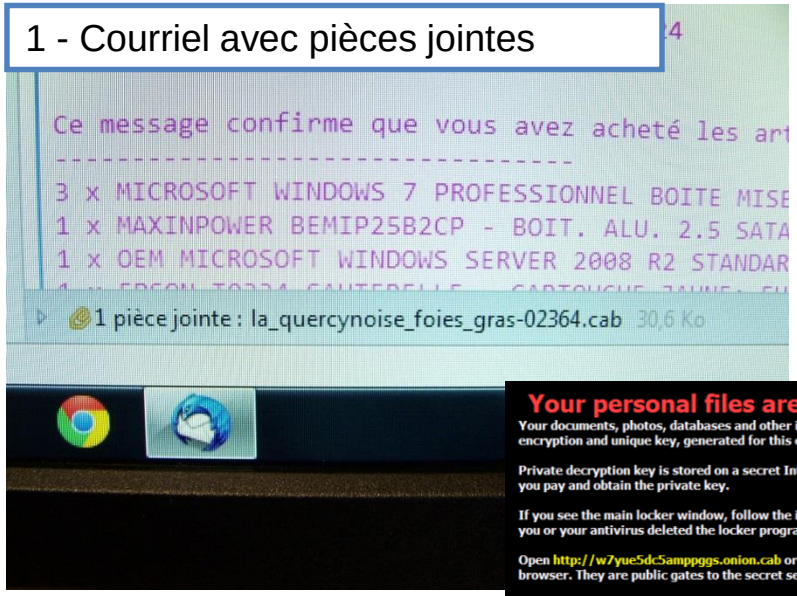
52 ransomwares différents

CYBERATTAQUES

Les Ransomwares (Cryptolocker)

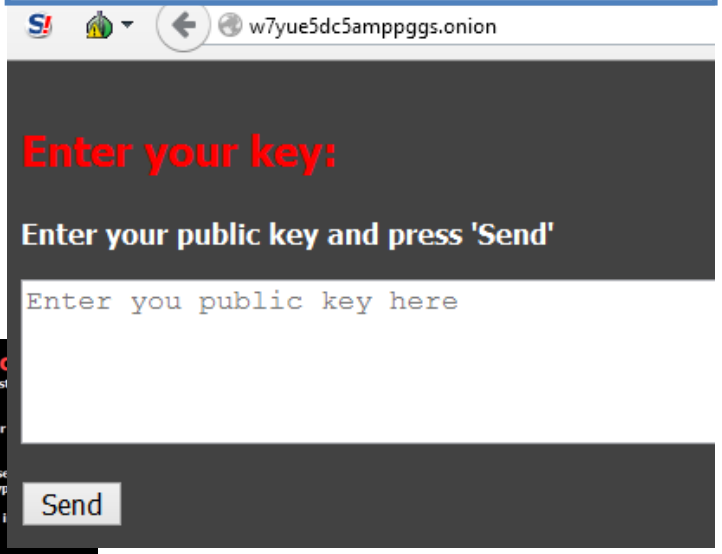
Janvier 2015

1 - Courriel avec pièces jointes



2 – demande de rançon

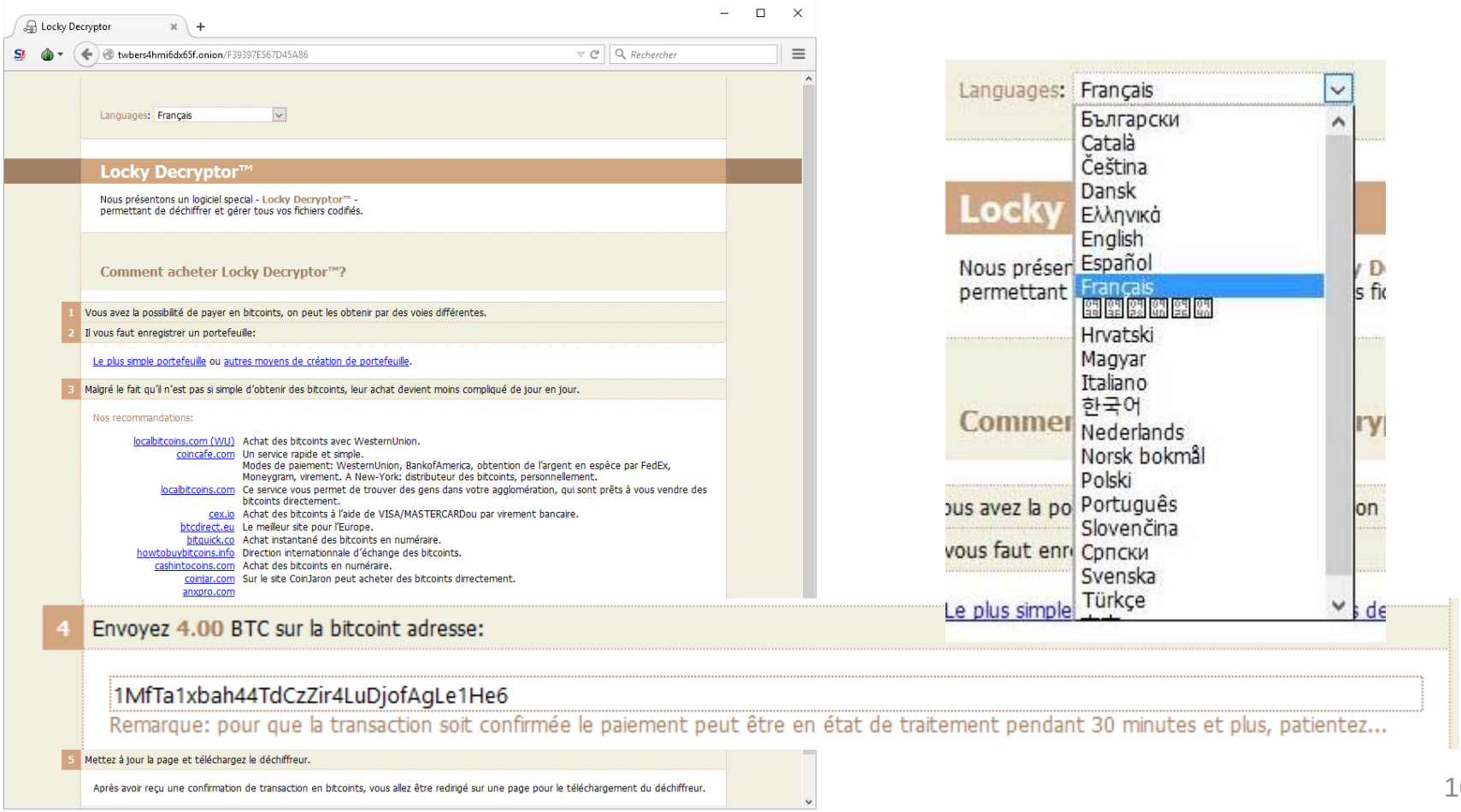
3 – Lieu de paiement



CYBERATTAQUES

Les Ransomwares (Cryptolocker)

Janvier 2016



Recommandations

L'arnaque au président

Les Ransomwares (Cryptolocker)

CYBERATTAQUES

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**.

CYBERATTAQUES

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 **Aeropspace valley**
- **Réserve Citoyenne Cyberdéfense** (**RCC**)

CYBERATTAQUES

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.

CYBERATTAQUES

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

CYBERATTAQUES

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

CYBERATTAQUES

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**

CYBERATTAQUES

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 »

CYBERATTAQUES

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 **Aeropspace 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-Pyrenées**

Echelon régional (3)

N-Tech

SAJ (1) - Assistances, Formations, Interventions et Audits de procédures

SR (2) - Direction d'enquêtes en cybercriminalité

Echelon Départemental (8)

BR – BDRIJ – CIC – Assistances aux unités

Echelon Elémentaire (200)

Correspondants N-Tech

BT – Assistances aux enquêteurs

Dépôt de plainte

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