

Les ransomwares

www.cert-ist.com



1^{er} décembre 2016

Martine GIRALT

THALES



Plan de la présentation

- ❖ Le Cert-IST
- ❖ Qu'est-ce qu'un ransomware ?
- ❖ Les cibles des ransomwares
- ❖ L'évolution des ransomwares
- ❖ Les impacts
- ❖ Les moyens de protection
- ❖ L'initiative « No more ransom »
- ❖ Conclusion
- ❖ Questions / Réponses

Industrie Services Tertiaire

Le Cert-IST



Présentation du Cert-IST

CERT : Computer Emergency Response Team

Prévention et support aux incidents

- Etre informé des nouvelles vulnérabilités,
- Identifier les nouvelles menaces et pouvoir s'en protéger
- Recevoir du support en cas d'incident



Offre Threat Intelligence

- Veille sur les Vulnérabilités
- Veille sur la menace (veille media, ...), attaques en cours, IOC, ...
- Support aux traitements d'incidents
- ...




Fondé et membre du FIRST
depuis
1999

Plus de
1 900
produits suivis et
16 000
versions

Environ
15
Dangers potentiels et
2 crises majeures
par an

Industrie Services Tertiaire

Qu'est-ce qu'un ransomware ?



Qu'est-ce qu'un ransomware ?

- ❖ Les ransomwares (ou rançongiciels) sont des logiciels qui :
 - bloquent un système (ordinateur, site web, téléphone mobile, ...) voire même une entreprise
 - demandent une rançon (souvent en crypto monnaie) pour le débloquer



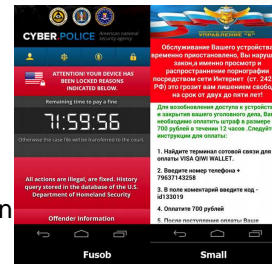
- ❖ Ils sont généralement utilisés par des cybercriminels pour :
 - gagner beaucoup d'argent
 - sans trop d'efforts
 - sans prendre des risques inconsidérés

- ❖ Nota : les logiciels utilisés pour bloquer un système peuvent également être utilisés pour le détruire (sans demander une rançon = sabotage)

Industrie Services Tertiaire

❖ On distingue différents types de ransomware :

- « Encryption Ransomware » qui **chiffre** les données
Ex. : **crypto-locker**, ..., **Locky**, et leurs nombreuses variantes
- « Lock Screen Ransomware » qui **bloque** l'utilisation d'un système cible Ex **Reveton**
- « Master Boot Record (MBR) ransomware » qui **modifie** le processus de boot Ex. **Petya**, **Satana**
- « Ransomware encrypting web server » qui **cible** les serveurs web et **chiffre** quelques fichiers
Ex. : **Rex** : ransomware web infectant les systèmes Linux et qui **change** les identifiants des administrateurs et demande une rançon pour déverrouiller l'accès au contenu du site (2016)
- « Mobile device ransomware » qui **bloque** l'utilisation d'un mobile (Android)
Ex. : **small** et **Fusob**



Industrie Services Tertiaire

❖ Les ransomwares utilisent différentes techniques pour atteindre leurs cibles :



- via des mails ou des clefs USB comportant des fichiers piégés (fichiers exécutables, image, winrar auto-extractibles,)
- Via des pages web piégées par des kit d'exploit (drive by download)
- Via des campagnes de publicité malveillantes (malvertising) qui invitent à aller visiter des pages web piégées
- Via de fausses applications mobiles
- ...



Industrie Services Tertiaire

Les cibles des ransomwares



Les cibles des ransomwares

❖ Au départ, les particuliers étaient les cibles privilégiées.

❖ Aujourd'hui, les entreprises, les services publics, les administrations, ... sont les nouvelles cibles

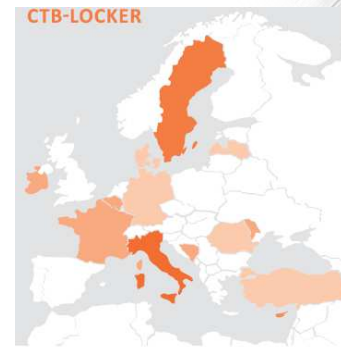
- Les hôpitaux (**Hollywood Presbyterian Medical Center**, ...)
- Les infrastructures industrielles (**BWL centrale hydro-électrique américaine – 2016**, **aciérie allemande – 2014**, ...)
- Les services publics (**les tramways de la ville de San Francisco** les 25/26 nov. 2016, ...)
- Les TPE/PME
- ...



En ciblant les entreprises, les services publics, les administrations, ... les rançons sont de plus en plus élevées.

Industrie Services Tertiaire

- ❖ Certaines campagnes de ransomwares ciblent plus certains pays que d'autres.
- ❖ Les attaquants peuvent changer de cibles / pays au fil du temps.



Industrie Services Tertiaire

L'évolution des ransomwares

❖ Les ransomwares constituent la menace informatique qui a connu l'essor le plus rapide :

- L'ancêtre des ransomwares est apparu en **1989 (Patient zero : Disquette AIDS)** mais leur essor date de **2005**
- Les ransomwares évoluent de plus en plus vite (variantes) pour échapper aux mises à jour des outils de détection...



Industrie Services Tertiaire

❖ Les ransomwares sont de plus en plus perfectionnés

❖ Mais, ils peuvent être utilisés par des individus de moins en moins qualifiés qui :

- utilisent des logiciels (Ex. **Tox**), pour créer leur ransomware,
- achètent ou louent les ransomwares avec des services de support
- Reversent parfois une part de leur bénéfice aux créateurs

=> **Ransomware-as-a-Service (RaaS)**

Ex. **Cerber**



Industrie Services Tertiaire




- ❖ En **2016**, « l'année du Ransomware », 4 fois plus de ransomwares ont déjà été détectés par rapport à 2015 !
- ❖ Selon le FBI, ils ont permis l'extorsion de **50 M\$** en 2015 et la prévision pour 2016 est de **+ de 1 000 M\$**
- ❖ Les ransomwares sont aujourd'hui l'une des armes préférées des cyber-criminels (la façon la plus simple de gagner de l'argent)
- ❖ C'est désormais l'une des principales cyber menaces en Europe

Europol 2016 <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016>

Industrie Services Tertiaire

Les impacts



The image shows a large iceberg floating in the ocean. The tip of the iceberg is visible above the water, while the much larger part of the iceberg is submerged below the surface. This visual metaphor represents the 'visible' vs. 'invisible' impacts of a security incident.

Financiers
Directs : paiement éventuel de la rançon
Indirects : arrêt de l'activité (1 semaine de non fonctionnement pour un hôpital), ou impossibilité de facturer les services (un jour pour les tramway de LA,)

Atteinte à E-reputation
L'image de marque de l'entreprise est automatiquement et durablement impactée

Juridiques
Un tiers peut se retourner contre l'entreprise victime si :
• Ses données ont été perdues ou si cela a perturbé son fonctionnement
• Le non fonctionnement d'un système a eu des conséquences sur lui (cas des hôpitaux, ...)

...

Computer Emergency Response Team
Industrie Services & Tertiaire

Cert-IST 2015

page 17

Les moyens de protection



❖ Pas de recette miracle mais l'application des mesures d'hygiène informatiques classiques ...

- Avoir une **politique de sécurité**, l'appliquer et la mettre à jour régulièrement
- **Sensibiliser** encore et toujours les utilisateurs mais partir de l'hypothèse qu'il y aura toujours un utilisateur qui ouvrira une pièce jointe
- Faire des **sauvegardes** régulières hors ligne
- Tester régulièrement les sauvegardes (restauration des données)
- **Patcher, patcher et encore patcher**



Industrie Services Tertiaire

❖ Pas de recette miracle mais l'application des mesures d'hygiène informatiques classiques ...



- Se tenir informé de l'évolution de la menace et adapter les mesures de détection et de protection
- Mettre à jour les outils sécurité (base de signatures,)
- Mettre en place un système de supervision et de détection et l'alimenter avec des IOC qualifiés
- bloquer certaines pièces jointes, interdire certains sites web (black list), restreindre la liste des applications,
- ...

Industrie Services Tertiaire

Que faire si on est victime d'un ransomware ?



Que faire si on est victime d'un ransomware ?

- ❖ Déconnecter immédiatement le poste du réseau (y compris wifi)
- ❖ Ne pas payer la rançon (cela ne garantit pas la récupération des données, n'interdit pas une nouvelle attaque et risque de compromettre le moyen de paiement)
- ❖ Utiliser l'initiative « No more Ransom » et/ou « ID Ransomware » et/ou les outils mis à disposition par certains éditeurs
- ❖ Restaurer les données sauvegardées après avoir réinstallé le système
- ❖ Comprendre le mode opératoire et mettre à jour les outils de détection et de prévention, la politique, ...
- ❖ Conserver les données chiffrées
- ❖ Porter plainte



Industrie Services Tertiaire

L'initiative

NO MORE RANSOM!



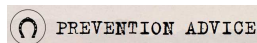
L'initiative

NO MORE RANSOM!

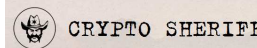
❖ Initiative lancée le 25 juillet 2016 par la police nationale des Pays-Bas, Europol, pour lutter contre les ransomwares
<https://www.nomoreransom.org/>

❖ Mise à disposition d'outils et d'informations pour :

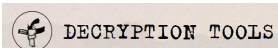
➤ Se protéger des ransomwares



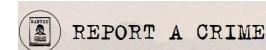
➤ Déterminer le ransomware



➤ aider les victimes à déchiffrer leurs données
(pour certains ransomwares)



➤ Porter plainte (en Europe ou aux Etats-Unis)



Industrie Services Tertiaire

Conclusion



❖ Les ransomwares vont-ils continuer à se développer et leurs techniques à évoluer?

- **Mc Afee Labs** prévoit qu'au 2^{ème} semestre 2017, les ransomwares seront moins nombreux et moins efficaces



« *Prévisions 2017 en matière de menace* » (Nov 2016)

<http://www.mcafee.com/fr/resources/reports/rp-quarterly-threats-sep-2016.pdf>

- **Kaspersky** prévoit l'émergence de « ransomware sale et menteur », sans restitution des données et donc une crise de confiance mais pas forcément une baisse des ransomwares.

Kaspersky Security Bulletin. Previsions 2017



<https://securelist.fr/analyse/kaspersky-security-bulletin/65752/kaspersky-security-bulletin-predictions-for-2017/>



❖ De nouvelles attaques vont-elles supplanter les ransomwares ?

- Les attaques DDOS (utilisant les Objets connectés)
- Les attaques sur les téléphones mobiles
- Les vols de données et/ou d'identités
- La destruction des données (sabotage)
- La désinformations (financière) Ex. [Vinci](#) en Novembre 2016
-



Questions / Réponses

