

SECURITE DES SYSTEMES D'INFORMATION**RANSOMWARE****Descriptif :**

Les rançongiciels illustrent des attaques actuelles consistant à empêcher que la victime ne puisse accéder à ses données (fichiers) personnelles.

Le malware va chiffrer ces données ou utiliser d'autres méthodes avant d'envoyer une demande de rançon en bitcoin.

Ces attaques peuvent être destinées à une victime isolée, à une entreprise (petite ou grande) ou à un Etat.

Le système d'exploitation de la victime n'est pas imposé.

Travail demandé :

Cette étude comprend les étapes suivantes :

- 1) Etude théorique & état de l'art
Comment fonctionne les rançongiciels ?
Quels sont les modes opératoires utilisés ?
Les malwares utilisés en 2016 sont-ils plus complexes que ceux de 2014 ?
Identifier sur internet des liens de qualité
Utiliser les excellentes publications de <http://www.miscmag.com/>
- 2) Mise en œuvre à partir d'un malware choisi
Quelles sont les techniques pour analyser son fonctionnement ?
Utiliser des outils appropriés pour :
 - Une exécution dans un bac à sable
 - Un monitoring du système de fichiers
 - Une analyse de type reverse engineering
- 3) Peut-on lutter efficacement contre ces rançongiciels ?

Sous réserve de modification en cours du projet de semestre

Candidat :

M. MANOUBI Yahia

Département : ITI

Professeur(s) responsable(s) :

Litzistorf Gérald

En collaboration avec :

Projet de semestre soumis à une convention
de stage en entreprise : non

Projet de semestre soumis à un contrat de
confidentialité : non