Projet de Semestre
Année Académique 2016-2017

Domaine: Sécurité des Systèmes d'information

Sujet: Les Ransomwares

h e p i a

Haute école du paysage, d'ingénierie
et d'architecture de Genève

Réalisé par : Manoubi Yahia

Professeur : M. Gérald Litzistorf

Table des matières

Enoncé……3

Introduction……4

I Etude Théorique et État de l'art……5
1.Etat de l'art……5
1.1 L'évolution des ransomwares……5
1.2 La Particularité des Ransomwares ……7
1.3 Les Ransomwares visent tous les OS……8
2. Mode de fonctionnement des ransomwares……9
2.1 La Diffusion ……10
2.1.1 Phishing email (hameçonnage)……10
2.1.2 Unpatched programs……10
2.1.3 Infected Softwares……10
2.1.4 Le Malvertising……11
a)Définition……11
b)Mode de Fonctionnement:……11
c)Comment se Protéger du Malvertising……13
2.2 L'infection……14
2.2.1 Comment sait-on qu'on est infecté……14
2.2.2 L'infection, mode de fonctionnement……15
2.2.3 L'Obfuscation……15
2.2.4 Que faire en cas d'infection……18
2.3 La Communication ……19
2.3.1 Domain Generation Algorithms……20
2.3.2 Chiffrement de la communication……20
2.3.3 Exemple d'échange entre un ransomware et son serveur C&C..20
2.4 La Recherche des Fichiers……21
2.5 Le Chiffrement……22
2.5.1 Introduction au chiffrement……22
2.5.2 La Cryptographie Hybride……22
2.6 La demande de rançon……23
2.6.1 L'évolution des modes de paiements……23
2.6.2 Le Pire des Cas (Le paiement)……24

II Mise en Oeuvre, Analyse et Monitoring d'un Ransomware……27
1. Méthodologie de travail……27
2. Environnement de travail……28
3.Lorobot……28
3.1 Le ransomware Lorobot……29
3.2 Exécution de Lorobot ……29
3.3 Analyse de Lorobot……30
3.3.1 L'infection……31
3.3.2 La diffusion……33
3.3.3 La communication……33
3.3.4 La recherche des fichiers……33
3.3.5 Le chiffrement……35
3.3.6 La demande de rançon……36
4. Les Packers……37
4.1 Etude Théorique……37
4.2 Etude Pratique……39
5. Locky……51
5.1 Le Ransomware Locky……51
5.2 L'exécution de Locky……52
5.2.1 Obfuscation et Packer……52
5.2.2 Exécution du binaire de Locky……53
5.3 L'analyse de Locky……53
5.3.1 La diffusion……54
5.3.2 L'infection……56
5.3.3 La Communication……57
5.3.4 La recherche des fichiers……60
5.3.5 Le Chiffrement……62
5.3.6 La Demande de Rançon……64
5.3.7 Résumé……66
III La Lutte Contre Les Ransomwares……68
1. La prévention……68
1.2 Prévention Basique……68
1.2 Prévention Avancée……69
1.3 Prévention pour les entreprises……73
2. La lutte contre les ransomwares, les perspectives……74

Conclusion……75

h e p i a

département I T I
ingénierie des technologies
de l'information

Année académique 2016-2017
Projet de semestre

Enoncé

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

Introduction

Le concept de la demande d'une rançon pour libérer des personnes prises en otages ou pour rendre des biens illégalement confisquées n'est pas nouveau. Tout au long de l'histoire humaine, de la Rome antique jusqu'à l'âge moderne de la piraterie et des enlèvements terroristes, les rapts, les prises d'otages ainsi que les mainmises sur les biens d'autrui ont une même stratégie et un stratagème commun. Aujourd'hui, les cybercriminels sont capables de distribuer, facilement, des attaques très efficaces, en utilisant des technologies de cryptage, initialement destinées à sécuriser nos systèmes informatiques, pour prendre des ressources numériques en otage, et ce, dans le but de monnayer leur libération et obliger leurs propriétaires à payer une rançon. En quelques années seulement, les cybercriminels, ayant opté pour ce type d'extorsion de fonds, ont développé une panoplie d'attaques, de celles de niche à la menace généralisée, affectant des réseaux de plus en plus nombreux

Pour mieux comprendre l'état actuel des ransomwares, nous devons examiner leur évolution, de leurs humbles débuts à la puissance qu'ils ont acquiert aujourd'hui. Leurs origines nous révèlent à quel point est arrivé l'un des problèmes cryptographiques les plus fastidieux d'aujourd'hui. C'est ce qui encourage les cyber-attaquants à les utiliser, d'une façon abusive et nous incite à mettre en œuvre tout ce qui est capable de nous assurer une meilleure protection de nos données.

Dans ce projet il s'agit, dans le cadre général de la sécurité des systèmes d'information, d'étudier les rançongiciels qui génèrent des attaques consistant à empêcher que la victime ne puisse accéder à ses données personnelles. Le malware chiffre ces données (ou bloque tout accès à elles) avant d'envoyer la demande d'une rançon payable, généralement en bitcoins. Ces attaques peuvent cibler une victime isolée ou une entreprise.
La première partie du rapport sera consacrée à l'étude théorique et l'état de l'art, dans laquelle j'expliquerai comment fonctionnent les rançongiciels en présentant les modes opératoires utilisés et je ferai une comparaison des malwares récents (apparus depuis 2014 tels que Locky, CryptoLocker and CryptoWall...) avec les plus anciens (existants avant 2014 tels que GpCode, Lorobot..).
La deuxième partie sera dédiée à la mise en œuvre du rançongiciel Locky, où j'expliquerai les techniques utilisées pour l'analyse du fonctionnement de ce malware, l'utilisation des outils appropriés pour une exécution dans un bac-à-sable et une analyse de type reverse engineering. Dans cette même partie j'expliquerai aussi les packers, leurs rôles, leur fonctionnement et les moyens de les contourner.
Dans la dernière partie du mémoire, je traiterai la problématique de l'exigence d'une lutte efficace contre les rançongiciels, j'exposerai les méthodes de prévention, les problèmes rencontrés et je terminerai par une conclusion.

CHAPITRE I Etude Théorique et État de l'art

1. Etat de l'art

Objectif: Dans ce qui suit, je présenterai les ransomwares, leur fonctionnement, leurs évolution, leur particularité et ce qu'ils visent comme OS.

1.1 L'évolution des ransomwares

Les Ransomwares ont existés, pendant des décennies, sous diverses formes, ils apparurent, pour la première fois, en décembre 1989. Le nombre d'attaques avec des ranconlogiels a connu une nette augmentation entre 2006 et 2007 à cause de l'apparition de plusieurs versions de GpCode. A partir de l'année 2010, de nouvelles variantes ont vu le jour utilisant de nouvelles techniques telles que l'utilisation des packers ; mais au cours de ces quatre dernières années, nous avons enregistrées des améliorations significatives qui ont été apportées et observée une nette augmentation du nombre des victimes touchées par ce malware.

Ce n'est qu'à partir de 2013 que les méthodes et autres techniques ont été déployées par les ranconlogiciels et dont voici une brève énumération:

- Le chiffrement fort (RSA, Courbes elliptiques, Diffie Hellman..) en 2013,
- L'algorithme de génération de domaine (DGA) en 2013,
- L'utilisation des serveurs C&C en 2013,
- L'utilisation du réseau anonyme TOR en 2014,
- Le vol des données bancaires en 2014,
- Le chiffrement des disques externes partagés en réseau.
- Le paiement par Bitcoins (2013).

Le tableau ci-dessous(Fig1), présente les ransomwares les plus connus depuis 1989 ainsi que les techniques et les méthodes utilisées par ces derniers. On remarque que chaque nouvelle génération de ransomwares s'appuie sur les points forts et corrige les erreurs des générations précédentes, comme par exemple famille de ransomwares Gpcode (entre 2004 et 2011) qui n'a pas cessé d'améliorer les faiblesses des versions précédentes et d'introduire de nouvelles techniques.

Ransomware	Date	Encrypts	Strng Cphr	PKI	Autonomy	DGA	HiddenTOR	HiddenI2P	HideClient	SecureEnc	SecureKeys	SecKeyMgmt	ScanNetDrv	SecErase	PK DL	DH-ECC	C2 Server	C2 Hidden	PayProcOK	PayPrvider	CryptCash	StealCred	StealProc
PC CYBORG	1989-12-19	√			√																		
One Half Virus	1994-10-31	√			√																		
GPcode	2004-12-01	√			√															√			
GPCode.ac	2005-06-27	√		o	√					x	x	x								√			
GPCode.ad	2006-04-14	√		o	√					x	x	x								√			
GPCode.ae	2006-06-02	√		o	√					x	x	x								√			
GPCode.af	2006-06-06	√		o	√					x	x	x								√			
GPCode.af2	2006-06-06	√	x	o	√					x	x	x								√			
GPCode.ag	2006-06-07	√	x	√	√					x	√	x								√			
GPCode.ak	2008-06-05	√	x	√	√					o	o	o								√			
GPCode.ax	2010-11-20	√	√	√	√					√	√	√							o	√			
GPCode.bn	2011-03-26	√	√	√	√					√	√	x							o	√			
Reveton.2012	2012-04-04				√												o		o	√			
Cryptolocker	2013-05-09	√	√	√		o				√	√	√	√		√		√		o	√	√		
Reveton.2013	2013-09-10				√												o		o	√			√
Reveton.XY	2013-10-22				√												o		o	√			
CryptoLocker 2.0	2013-12-19	√	√	√						√	√	√	√		√		√		o		√		
CryptoDefense	2014-03-26	√	√	√			o			√	√	x					√	o					
CryptoDefense	2014-04-01	√	√	√			o			√	√	√		o			√	o					
CryptoWall	2014-06-26	√	√	√						√	√	√	o		√		o		o		√		
CTB-Locker	2014-07-15	√	√	√	o		o			√	√	√	o		√	√	√		o		√		
Reveton.2014	2014-08-19				√												√		o	√	o	√	√
CryptoWall 2.0	2014-10-01	√	√	√			o			√	√	√	o		√		√	√	√		√		
CryptoWall 3.0	2015-01-14	√	√	√				√		√	√	√	o		√		√	√	√		√		
Reveton.2015	2015-02-05				√												√		o	√	o	√	√
TeslaCrypt 0.2.5	2015-02-14	√	√				√			√	√	x					√	√	x		√		
TeslaCrypt 0.4.0	2015-02-14	√	√		o		√			√	√	o	√	√			√	o	√		√		
TeslaCrypt 2.0.0	2015-07-13	√	√	√	o		√			√	√	o	√	√		√	√	√	√		√		
TeslaCrypt 2.1	2015-09-07	√	√	√	o		√			√	√	√	√	√		√	√	√	√		√		
√ = well implemented; o = not fully implemented; x = implementation broken																							

Fig1

Les mots clés:

Encrypts	Chiffrement des fichiers et pas seulement leurs bloqués l'accès.	**ScanNetDrv**	Chiffre les disque externe, les disques et les backups présent dans le réseau.
Strng Cphr	Utilise un chiffrement fort.	**SecErase**	Supprime en toute sécurité les fichiers originaux(non chiffrés).
PKI	Utilise une infrastructure à clés publiques(pub key/ pri key).	**PK DL**	Le serveur C&C transmet une clé publique au ransomware et garde la clé privée.
Autonomy	Ne nécessite pas une communication avec un serveur C&C pour commencer l'infection.	**DH-ECC**	"Diffie Hellman/Courbe elliptique" pour générer une paire de clés pub/pri, similaire à RSA.
DGA	L'algorithme de génération de domaine.	**C2 Server**	Communique avec un serveur Commande & Control (C&C).
HiddenTOR	Utilise le réseau anonyme TOR.	**C2 Hidden**	Le serveur C&C est caché dans un réseau anonyme(e.g TOR).
HiddenI2P	Utilise le réseau anonyme I2P(similaire à TOR).	**PayProcOK**	Utilisation d'un protocole de paiement sécurisé / transactions non falsifiable.

HideClient	La communication entre le ransomware et le serveur C&C est complètement chiffrée.	**PayPrvider**	Paiement effectué de façon anonyme(e.g e-gold, moneypak..)
SecureEnc	Une bonne implémentation des méthodes cryptographiques.	**CryptCash**	Paiement avec une monnaie cryptographique(Bitcoin).
SecureKeys	Impossible de déchiffrer les fichiers sans les clés de chiffrement(des longues clés de chiffrement, une clé pour chaque fichier..).	**StealCred**	Le ransomware essaye en plus de voler des données bancaire et des mots de passe.
SecKeyMgmt	Une bonne gestion des clés(aucune trace des clés de chiffrement, ni sur le disque, ni dans la mémoire).	**StealProc**	De plus le ransomware essaye de causer des dégâts dans le réseau local(vol de mots de passe)

D'autres parts, la prolifération de ce genre de malwares est due au fait que leur création n'est plus l'apanage des Hackers professionnels (qui ont des connaissances solides en programmation et en sécurité informatiques), car des outils de génération de ransomwares existent depuis peu sur le DeepWeb. Avec ces outils, un hacker, ayant des connaissances techniques élémentaires, peut rapidement assembler son propre rançonlogiciel personnalisé.

Lien: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1179&context=ism

1.2 La Particularité des ransomwares

Un Ransomware n'a pas la subtilité des chevaux de Troie les plus traditionnels qui cherchent à échapper à la détection et à voler des informations sensibles, comme les numéros de carte de crédit et les informations bancaires, ou qui cherche à se reproduire comme un virus ordinaire. Au lieu de cela, un ransomware rend immédiatement sa présence connue en chiffrant les fichiers et en exigeant le paiement des clés pour les déverrouiller/déchiffrer.

1.3 Les Ransomwares visent tous les OS:

Les ransomwares touchent quasiment tous les types d'OS, les PCs et les mobiles. La majorité des ransomwares qui attaquent les mobiles, touchent principalement les Androids, ces ransomwares sont des Blockers et non des crypto-malwares, qui sont simples et ne chiffrent pas les données mais bloquent l'accès de l'OS aux fichiers. D'autres parts, l'OS Android ne permet pas un accès total à tous les fichiers présents dans le mobile et les méthodes de chiffrement ne sont pas disponibles et exploitables.
En outre, les mobiles (IPhones et Androids) ont des fonctionnalités qui permettent de sauvegarder automatiquement les données sur le Cloud.
Apple ne détient que 7,4% des ordinateurs (Portables et bureautiques) produits dans le monde et ses OS (OS X..) dérivent des OS UNIX construits avec un mécanisme d'autorisation assez robuste qui empêche l'exécution non autorisée des logiciels. Un nombre très faible de ransomwares vise les plateformes de type Linux (Ordinateurs et serveurs).

Les PCs Windows se taillent la part du lion du marché mondial des ordinateurs. Les OS Windows présentent plus de failles et de vulnérabilités, que ceux cités dans le paragraphe précédent et sont, de ce fait, les plus visés par les ransomwares.
Pour ces raisons, je me propose, dans ce rapport, d'étudier, d'une façon détaillée, les ransomwares qui visent les pc Windows (Win7).

2. Mode de fonctionnement des rançongiciels:

Le schéma ci-après, donne une vue globale des 6 étapes du fonctionnement d'un ransomware, chaque étape sera détaillée par la suite.

Fig2

2.1 La Diffusion

2.1.1 Phishing email (hameçonnage):

Les emails prétendent être envoyés par des sites de réseaux sociaux populaires, de banques, ou des administrateurs informatiques, ils sont couramment utilisés pour attirer les victimes sans méfiance. Les courriels d'hameçonnage peuvent contenir des liens URL vers des sites infectés ou des liens URL qui dirigeront les victimes sur d'autres sites infectés.

Les emails prétendent être envoyés par des sites de réseaux sociaux populaires, de banques, ou des administrateurs informatiques, ils sont couramment utilisés pour attirer les victimes sans méfiance. Les courriels d'hameçonnage peuvent contenir des liens URL vers des sites infectés ou des liens URL qui dirigeront les victimes sur d'autres sites infectés.

2.1.2 Unpatched programs:

Les attaques exploitent les vulnérabilités côté client dans des programmes couramment utilisés tels qu'Adobe PDF Reader, QuickTime, Adobe Flash et Microsoft Office.Ces vulnérabilités côté client sont exploitées par les attaquants lorsque les utilisateurs visitent des sites Web infectés, les visiteurs se sentent en sécurité pour le téléchargement de documents à partir des sites de confiance.

2.1.3 Infected Softwares:

Les Logiciels gratuits téléchargés à partir de sites webs infectés ou à partir de logiciel de téléchargement *peer-to-peer,* dans ces cas d'attaques le Hacker empaquette son malware (Ransomware dans notre cas) avec un autre Logiciel légitime qu'il propose dans un site ou dans les forums, l'utilisateur pensant télécharger un logiciel cracké gratuitement télécharge aussi le Malware, ce dernier s'il est en mode Administrateur verra s'afficher une fenêtre le prévenant de la provenance inconnue du Logiciel (après la demande d'élévation de privilèges) en cours d'exécution, mais souvent l'utilisateur clique sur "OK".

2.1.4 Le Malvertising:

Objectif: Ici, il sera question de souligner le caractère pernicieux de ce concept nouveau, en explicitant son mode de fonctionnement, le drive-by-download comme méthode utilisée et la façon de se protéger contre lui.

a) Définition :

Le *malvertising* est un moyen relativement nouveau(après 2014) pour la diffusion de logiciels malveillants et surtout difficile à combattre, car il peut faire son chemin dans une page Web et se propager à l'ordinateur d'un internaute à son insu, le problème majeur avec les infections par *malvertising* est qu'ils ne nécessitent aucune action de la part de la victime pour infecter son ordinateur(même pas un clic), les infections livrées par *malvertising* voyagent silencieusement à travers des pages Web légitimes à l'insu de leurs propriétaires.
Pour ces raisons, ce nouveau mode de diffusion sera le mieux expliqué dans ce rapport.

b) Mode de fonctionnement:

Le Malvertising a impliqué récemment des sociétés dignes de confiance (comme le site web du New York Times, de la BBC, Yahoo..). Souvent, les hackers placent des publicités "propres" dans des sites dignes de confiance en premier lieu afin de gagner la confiance de l'hébergeur et des visiteurs, ensuite ils mettent à jour (à distance) l'annonce qui injecte le logiciel malveillant (des pubs qui tournent sur Adobe Flash ou Sliverlight par exemple) infectant ainsi tous les visiteurs du site pendant une certaine période. Les identités des responsables sont souvent difficiles à tracer, ce qui rend difficile de prévenir les attaques ou de l'arrêter complètement, car l'infrastructure des réseaux publicitaires est très complexe avec plusieurs intermédiaires entre les annonceurs présumés et l'hébergeur de la publicité.

La méthode utilisée est le 'drive-by-download'. En premier lieu:
(0) Le client accède à un site qui pourrait héberger une pub malicieuse.
(1) Un script initial (pas malicieux pour le moment) vérifie qu'il n'est pas exécuté dans un environnement contrôlé (monitored environment) afin d'échapper à l'analyse des chercheurs.
(2) Ce même script collecte des informations sur la PC de la victime potentielle, comme la version du logiciel Flash et des autres plug-in du Browser qui peuvent contenir des failles de sécurité, et les transmet au serveur distant de l'attaquant, ces serveurs sont basés sur un modèle Server-Side Logic (l'intelligence et les traitements se font du côté serveur dans la relation Client-Serveur).
Donc en fonction des informations collectées, le serveur de l'attaquant qui héberge la bannière publicitaire, (3) transmettra une bannière propre si le serveur ne dispose pas d'un exploit kit correspondant à la version du navigateur et des plugins installés sur le pc cible ou si un logiciel d'analyse/Sniffer/SandBox/Machine Virtuelle est détecté, dans le cas contraire, (4)une bannière malicieuse est envoyé au client, c'est une bannière "mascarade", elle a la même

apparence que la pub propre, mais contient une URL de redirection (silent https redirect)(5), cette URL est chiffré ou réduite de type Tiny télécharge(6) le exploit kit sur le PC de la victime, les Exploit Kit les plus utilisé sont Angler et Neutrino, les derniers ransomwares utilisant des images publicitaires utilisent souvent Stegano.

(7) Lors d'une exploitation réussie, un code shell (différent du script initial) est exécuté, recueille des informations sur les produits de sécurité installés et effectue un autre contrôle pour vérifier s'il est surveillé ou non.

(8) Si les résultats lui sont favorables, il essaiera de télécharger la charge utile cryptée d'un serveur distant (l'exploit kit et la charge utile du ransomware peuvent être stockés dans le même serveur) déguisée en une image gif.

(9) La charge utile est téléchargée pour être, ensuite, déchiffrée.

(10) Le malware est lancé via un processus légitime, par exemple regsvr.exe ou rundll.exe. Les charges utiles détectées à ce jour incluent les backdoors, les trojans bancaires, les spywares, et les ransomwares.

Le Schéma ci-dessous(Fig3) montre une infection typique de type malvertising que les nouveaux ransomwares utilisent:

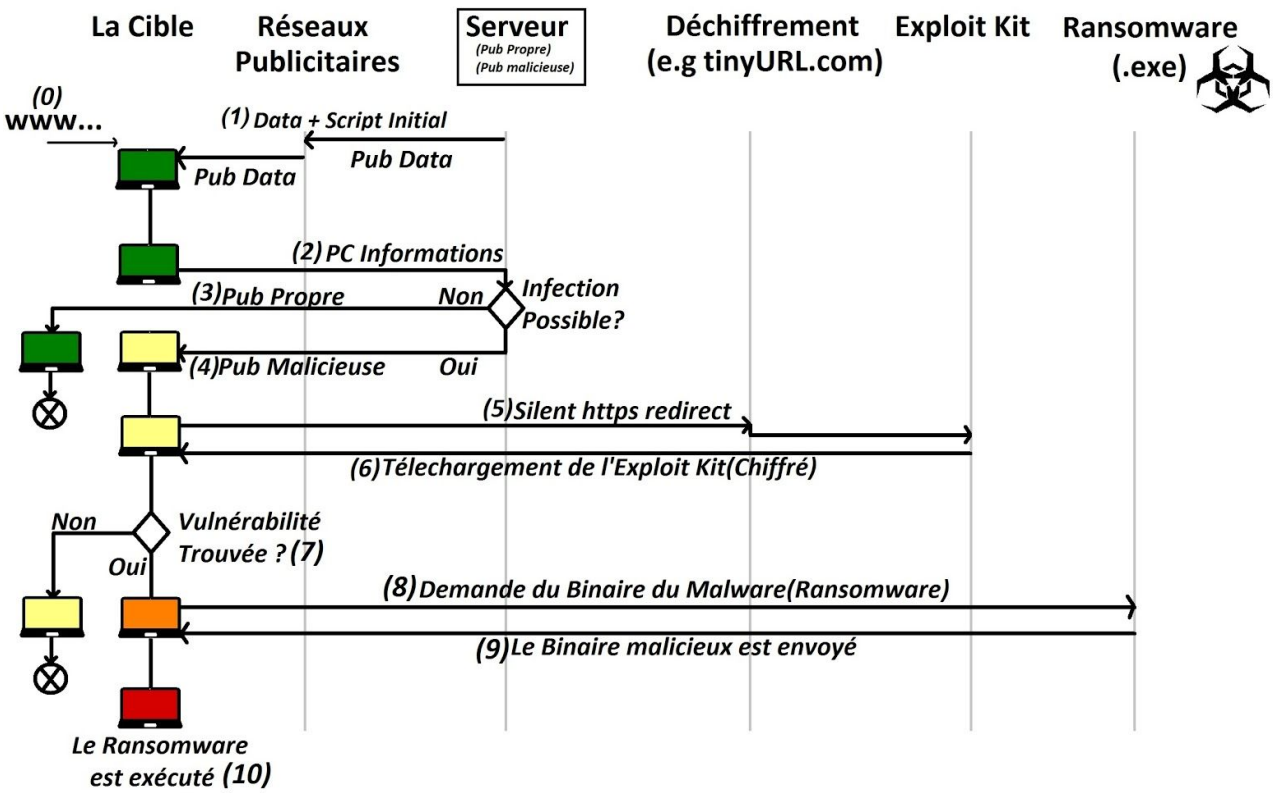


Fig3

c) Comment se protéger du Malvertising:

- Désactivation d'Adobe Flash dans le navigateur. Les annonces malveillantes peuvent utiliser des vulnérabilités dans Flash pour installer des logiciels malveillants. Cela pourrait affecter certaines fonctionnalités de sites Web.□HTML 5 commence à remplacer Flash, car du point de vue sécurité, il est plus sûr, son utilisation pourrait donc limiter les dégâts, mais il se trouve, malheureusement, que son langage de base est Javascript, et que l'une des techniques sur lesquelles se base le malvertising est l'injection d'un code JavaScript malicieux, il peut en résulter donc qu'un script malveillant soit emballé dans HTLM5 sans beaucoup de difficulté.□Nous pouvons conclure que les versions actuelles de HTML 5 ne seront pas une solution complète contre le malvertising, des améliorations doivent être apportées au niveau du langage, tel qu'un HTML 6 avec de meilleurs codecs et qui se base sur un autre langage comme Python. Cela pourrait améliorer considérablement la lutte contre le malvertising.□□

- Suppression ou désactivation de Java et Silverlight. Cependant, de nombreux sites Web s'appuient encore sur java pour fonctionner. □□

- Si un utilisateur ne désire pas désactiver Flash et Java, l'activation des plug-ins "Click-to-Play" est, dans ce cas, fortement recommandée. Grâce à ces plug-ins et lorsqu'un utilisateur visite une page web contenant un objet Flash ou Java, ce contenu n'existera pas automatiquement car il faudra cliquer dessus pour l'activer. □□

- Suppression ou désactivation des plug-ins que vous n'utilisez pas fréquemment, cela réduirait le nombre des vulnérabilités exploitables par une attaque.□□

- L'utilisation d'un logiciel Anti-exploit comme "Malwarebytes anti-exploit", ce genre de software n'est pas un antivirus mais il peut fonctionner conjointement avec un antivirus, il surveille les navigateurs web et leurs plug-in afin de détecter et de bloquer automatiquement les exploit-kit.

- L'utilisation de bloqueurs d'annonces, particulièrement utilisé dans un environnement d'entreprise, peut être efficace (par exemple Adblock).

- L'activation de la mise à jour automatique des plug-ins, et des navigateurs web.

- Voir les bonnes pratiques dans le Chapitre III.

Lien Malvertising:
https://blog.malwarebytes.com/cybercrime/exploits/2016/12/adgholas-malvertising-business-as-usual/

https://blog.malwarebytes.com/101/2016/06/truth-in-malvertising-how-to-beat-bad-ads/

2.2 L'infection

2.2.1 Comment sait-on qu'on est infecté:

- Vous ne pouvez pas soudainement ouvrir vos fichier ordinaires, en double cliquant sur un fichier ou un dossier vous obtenez un message d'erreur telles que: "Mauvaise extension" ou "le fichier est endommagé".

-Au lieu de votre fond d'écran habituel, un autre Desktop crée et avec une autre image de fond d'écran vous alertant que vos fichier sont désormais chiffrer et qu'il faut payer une rançon pour les récupérer, ce nouveau Desktop persistant est créé avec la fonction *CreateDesktop* de *WinAPI.*

-Une fenêtre s'affiche, et qui ne ferme pas, contenant le même message que l'image de fond d'écran précédente.

-Sur votre Bureau il y a des nouveaux fichiers par exemple: HOW_TO_DECRYPT_FILES.TXT ou DECRYPT_INSTRCUTIONS.HTML.

Exemple de Fenêtre d'une demande de Rançon (CryptoLocker, 2013)

Fig4

2.2.2 L’infection, mode de fonctionnement:

Les ransomwares, à l'instar des malwares récents, ne se contentent plus d’attaquer et de causer des dégâts dans la machine/réseau infecté mais ils se défendent aussi, ils cherchent, pendant les phases d’infection et d'exécution, à échapper à toute détection ; après l'exécution et le chiffrement des fichiers, ils rendent leur présence visible pour la victime. □
Une infection commence par le lancement du fichier malveillant exécutable, dans la plupart des cas, le code est protégé avec un Packer, c’est un paqueteur qui chiffre et compresse une ou plusieurs fois un code malveillant (dans la partie II du rapport, un paragraphe entier sera consacré à l’analyse du fonctionnement des packers.) En plus de l’utilisation des packers, le code source des ransomwares est obfusqué.

2.2.3 L’Obfuscation:

Objectif: Il s’agit de montrer comment la technique de l’obfuscation est utilisée, à la fois, par les développeurs de logiciels légitimes et par les créateurs des ransomwares ; ces derniers cherchant, sans cesse, à sophistiquer leurs stratagèmes.

L'obfuscation est une technique de défense contre le reverse engineering et l’analyse de code qui rend illisibles le/les code(s) source d’un programme et/ou difficiles à comprendre. Les développeurs de logiciels légitimes emploient parfois des techniques d'obfuscation pour empêcher que leurs programmes ne soient désassemblés ou piratés.

Pour les malwares, il est primordial de cacher des mots et des instructions clés utilisés, tels que des URL ou des appels de fonctions suspectes (comme les API utilisés dans les injections DLL ou le chiffrement), car ils donnent un aperçu du comportement du logiciel malveillant. Dans le monde des ransomwares, des malwares, tels que GpCode, vont plus loin et protègent leurs binaires avec un programme spécial appelé packer (le packer UPX de GpCode sera analysé en détail dans la partie II du rapport.)

La mise en œuvre de l’obfuscation peut être simple, comme par exemple, en utilisant :

- De simples manipulations de bits.
- Des rotations.
- L’application de l'opération XOR une ou plusieurs fois.
- Le codage en Base64.

Elle peut être avancée avec des méthodes cryptographiques tels que DES, AES…

Exemple: Ici un exemple d'Obfuscation avec une seule opération XOR, cette méthode est simple à implémenter et très utilisée par les créateurs des ransomwares,

Données chiffrées (illisibles)

Les mêmes données déchiffrées avec une opération XOR (clé=0x55)

On remarque la présence d'une URL malveillante, ce malware essayera de contacter "http://tator1157.hostgator.com" pour récupérer le fichier exécutable "bot.exe".

Les auteurs des ransomwares savent que ce type de chiffrement n'est pas robuste et que les antivirus arrivent facilement à déchiffrer les binaires chiffrés avec une simple opération XOR, ces derniers applique plusieurs XOR avec des clés différentes sur le même code, ou en utilisant une suite de clés bien déterminé pour contourner les programmes de détection d'XOR, la détection par les signatures statiques, tromper l'analyseur heuristique, et les Antivirus.

L’infection, mode de fonctionnement:(Suite)

L’infection commence par le lancement du fichier (malveillant) exécutable, dans la plupart du temps le code est protégé comme on a vu avec un packer.

Une fois décompressé et déchiffré, le ransomware injecte une DLL malveillante (Setup.dll) dans une zone de RAM d’un processus légitime, puis lui passe le contrôle, l’injection DLL consiste à injecter un code malveillant, depuis le processus créé par le ransomware dans la RAM, dans une zone mémoire d’un autre processus légitime qui tourne déjà sur le système, souvent c’est les processus “explorer.exe” et “svchost.exe” qui subissent de telles injections. Pour que deux processus puissent communiquer, ils doivent avoir le même niveau de sécurité, le processus du ransomware doit donc avoir le même niveau de sécurité que le processus qu’il compte corrompre, pour cela, plusieurs options sont possibles, une demande d’élévation de privilège peut être faite à l’utilisateur, si ce dernier a des droits Admin et qu’il accepte la requête UAC pour une *Élévation des privilèges,* le processus malveillant monte à un niveau supérieur de sécurité.
Une autre possibilité consiste à exploiter une faille dans le système d’exploitation de Windows semblable à l’attaque *Shatter Attack* (Win XP, Win2000)*,* ces exploits peuvent entraîner une escalade de privilèges. Une fois le code du processus légitime dans la mémoire est corrompu, le binaire (.exe) du ransomware s'autodétruit pour ne laisser aucune trace sur le disque, laissant le code injecté dans la mémoire RAM faire le reste.

La succession et la sophistication des étapes suivantes diffèrent légèrement d’un ransomware à un autre, mais d’une manière générale, les ransomwares essayeront d’effectuer les opérations suivantes:

- La génération d’un identifiant unique pour le PC infecté, cet ID sera utilisé pour identifier la clé de déchiffrement correspondante à chaque PC infecté dans les serveurs des attaquants.
- L’infection de la MBR (Master Boot Record) afin d'empêcher le chargement normal du système d’exploitation lors du redémarrage, l’infection consiste à déplacer la MBR ailleurs dans le disque, de telle façon que le code du ransomware s'exécute en premier lorsque le BIOS essaye de charger le système d'exploitation lors du démarrage du PC. Certains Ransomwares (Peyta par exemple) crypte la MBR.
- D’autres ransomwares, pour assurer leur lancement lors du démarrage, ne touchent pas à la MBR mais essayent de s'exécuter en AutoRun en Modifiant les valeurs de certaines clés de la Base de Registre.

- Le chiffrement de la MFT (Master File Table), c'est la table de fichiers principale, son chiffrement bloque le fonctionnement normal du système de fichiers NTFS et l'accès normal aux fichiers sur le disque dur.
- La désactivation du service "Volume Shadow Copy" (VSS), qui fait des back-up automatiques.
- La désactivation des services "Start-up repair" , "Windows error recovery", "Windows Security Center" , "Windows Defender" , "Windows Update Service" , "Error Reporting" , "BITS"(Background Intelligent Transfer Service).

2.2.4 Que faire en cas d'infection:

Si vous vous estimez victime d'une attaque de type Ransomware (ou si vous avez des doutes), il faudra prendre immédiatement les mesures suivantes:

1) La Déconnexion:
   - Déconnectez immédiatement l'ordinateur infecté de tout réseau sur lequel il est connecté.
   - Désactiver toutes les fonctionnalités sans fil tels que Wi-Fi ou Bluetooth. - Débranchez tous les périphériques de stockage tels que les disques durs USB ou externes.
   - Ne pas effacer ou "analyser" les fichiers/Dossiers infectés avec des antivirus.
2) L'estimation des dégâts:
   Faire un inventaire des périphériques/structures de stockages compromis ou Chiffrés (dossiers partagés, stockage réseau de toute nature, disques durs externes, clés USB, stockage en Cloud..).
3) La Collecte d'informations:
   - Il est important de savoir exactement avec quel ransomware vous faites affaire, il faudra noter toutes les informations possibles sur le ransomware(Version, comment on l'a téléchargé..)

   -Essayer de créer des paires contenant des fichiers non chiffrés(depuis DropBox, Google Drive) et les même fichiers chiffrés, des couples "Fichier chiffré/ Fichier clair" sont utile pour des services de déchiffrement.

   La chance de déchiffrer les fichiers infectés par des ransomwares récents est faible, mais plus considérable pour des anciens ransomwares. il est possible de trouver des outils de déchiffrement développer par des entreprises de sécurité informatique qui essaieront de déchiffrer vos fichiers sans avoir à payer.
4) La Décision:
   Une fois la portée et les dégâts causés par le ransomware ainsi que son type connu, il vous reste plus qu'à entre ces options:

- Restaurer vos données à partir d'une sauvegarde récente.
- Décrypter vos fichiers avec un décrypteur tiers (c'est une chance très mince).
- Ne rien faire (vous perdrez vos données).
- Négocier / Payer la rançon.

Souvent la première réactions d'un utilisateur c'est de démarrer une analyse de son système avec un antivirus ou d'installation d'un Anti-Ransomware, si cette analyse est lancé lorsque le PC est déconnecté et que Ransomware a chiffré un certain nombre (ou la totalité)des fichiers mais qu'il n'a pas encore communiqué avec les serveurs pour leurs transmettre par exemple la clé de chiffrement utilisée et des informations sur le PC(son ID..). Dans ce cas, l'analyse par l'antivirus peut entraîner la suppression du binaire du ransomware ce qui signifie qu'il ne sera plus possible de récupérer les fichiers par le paiement de la rançon, par ces lignes je n'encourage pas le paiement des rançons mais plutôt pour expliquer ce que peut entraîner techniquement une telle action.

2.3 La Communication

Dans certains cas de ransomwares, cette étape suit l'étape de chiffrement, ce sont les ransomwares autonomes, ils n'ont pas besoin d'une commande particulière de la part d'un serveur distant pour commencer l'infection d'un pc cible.

Jusqu'à 2009, la communication n'était pas un élément essentiel dans le plan d'attaque de certains ransomwares qui ne communiquaient pas….certains ne communiquaient pas avec des serveurs distants, ils s'exécutent et chiffrent les fichiers d'une façon autonome, ensuite ils demandent à la victime de contacter le ravisseur, par email, pour recevoir les instructions de paiement.

Les premiers ransomwares contactaient un serveur distant grâce une URL précise, codé en dur dans le code source du malware. Il était alors facile pour les autorités de contacter l'ISP pour faire fermer le serveur. Les machines infectées par ransomware seraient incapables alors de d'échanger des clés et d'envoyer des données utilisateur au serveur. Pour conteourner ça, les hackers placent leurs serveurs dans les réseaux anonyme tel que TOR ou I2P, et utilisent des techniques tel que la DGA.

2.3.1 Domain Generation Algorithms

La technique DGA est utilisée car les logiciels malveillants qui dépendent d'un domaine fixe ou d'une adresse IP sont rapidement bloqués. Donc, plutôt que d'apporter une nouvelle version du logiciel malveillant ou de configurer tout, à nouveau, sur un nouveau serveur, le logiciel malveillant génère périodiquement(à intervalles réguliers) un grand nombre de noms de domaine pouvant être utilisés comme points de rendez-vous avec leurs serveurs de C&C.

2.3.2 Chiffrement de la communication

Nous pouvons identifier au moins deux objectifs principaux pour déployer le chiffrement dans la communication entre le système compromis et C & C:

- Échapper à la détection.
- La confidentialité.

Les nouveaux ransomwares adoptent des normes de chiffrement que TLS. Cela rend la détection proactive du trafic d'un réseau beaucoup plus difficile car il n'est pas du tout aisé de distinguer si le chiffrement est en place pour sécuriser les communications légitimes, comme les services bancaires sur le Web, ou s'il est utilisé pour masquer la communication avec les C & C.

Lorsqu'une communication C & C est chiffrée, la détection au niveau réseau requiert que le réseau de la victime dispose de capacités supplémentaires afin d'inspecter le trafic.

Dans les cas où le réseau ne dispose pas d'une telle capacité, les logiciels malveillants, utilisant le chiffrement pour établir une connexion avec son serveur C & C, seront exécutés sans être détectés jusqu'à ce que les C & C soient découverts et ajoutés aux listes noires d'adresses IP et de domaines malveillants.

Par conséquent, ce type de protection est surtout réactif.

2.3.3 Exemple d'échange entre un ransomware et son serveur C&C

Voici un échange typique simplifié entre un ransomware et son serveur C&C:

- Le ransomware compromet le système de la victime et notifie son serveur C & C avec un ID unique et d'autres informations sur le système infecté.
- C&C répond par un OK pour confirmer la réception des informations,
- Le ransomware envoie une requête pour demander une clé publique.
- C&C répond avec une clé publique d'une paire RSA-1024/2048 créée de façon unique pour cette ID unique.
- La clé privée ne quitte jamais le serveur C & C.
- Le ransomware acquitte la réception de la clé publique au serveur C&C.
- Le ransomware envoie les clés utilisées dans le chiffrement des fichiers au serveurs(ces clés sont chiffrées avec la clé publique).

- Le ransomware notifie au serveur que le processus de chiffrement est terminé.

Liens:
DGA:https://blog.malwarebytes.com/security-world/2016/12/explained-domain-generating-algorithm/
Communication:http://www.welivesecurity.com/2016/09/13/how-encryption-molded-crypto-ransomware/
I2P/TOR:https://www.ivpn.net/privacy-guides/an-introduction-to-tor-vs-i2p

2.4 La Recherche des Fichiers

Dans cette étape, le ransomware essaie de répertorier le maximum de disques dur et de systèmes de stockage à partir du pc hôte, les ransomwares récent sont capable de collecter quasiment de toute sorte de mémoire connectée directement au pc hôte(Disques dur: C: D:.. SSD, USB..) ou se situant dans son réseau locale et des espaces de stockage pour Backup(VSS..), ainsi que les dossiers partagés.
En fonction de la complexité du ransomware, il pourrait ensuite créé un thread pour chiffrer chaque zone mémoire détecté ou les chiffrer dans le main() du programme principale de façon séquentielle.
La quasi majorité des ransomwares ont une liste des extensions des fichiers qu'ils ciblent, cette liste est codée en dur dans le code source du malware, en moyenne cette liste contient une bonne centaine d'extensions. les ransomwares récent prennent le soin de ne pas chiffrer les fichier indispensables au bon fonctionnement de l'OS.

2.5 Le Chiffrement

2.5.1 Introduction au chiffrement

En tant que technique, le chiffrement n'est pas intrinsèquement mauvais. En fait, c'est un outil puissant et légitime pour protéger les données contre l'accès non autorisé, un outil employé par les individus, les entreprises et les gouvernements. Tout comme n'importe quel autre outil informatique puissant, le chiffrement peut être mal utilisé, les ransomwares sont l'exemple d'une telle utilisation, utilisé de cette façon, le chiffrement et le déchiffrement des données est analogue à la prise des données en otage et ensuite, peut-être, à leur libération. Ainsi, le chiffrement est utilisé comme un moyen pour kidnapper les données des victimes et d'obtenir une rançon pour les libérer.

Le chiffrement est un élément clé des ransomwares, car son business plan entier dépend d'un chiffrement réussie des fichiers d'une victime (si les victimes n'ont pas de plans de récupération comme les sauvegardes des données).

Le chiffrement est également utilisé pour sécuriser la communication entre le logiciel malveillant et son serveur de commande et de contrôle (C & C), qui détiendra finalement une clé nécessaire pour déchiffrer des données ou récupérer la clé de déchiffrement nécessaire à la récupération des fichiers dans leurs formats non chiffrés .

2.5.1 La Cryptographie Hybride

Les principales raisons du chiffrement hybride sont la performance et la commodité. Le chiffrement symétrique et asymétrique sont combinés afin d'obtenir le meilleur des deux méthodes.
Les ransomwares qui utilisent cette méthode, fonctionnent comme suit :
Une clé aléatoire est générée localement coté pc infecté par un algorithme à clé symétrique appelée Clé de session, elle sera utilisée pour chiffrer les fichiers, cette clé est ensuite chiffrée avec un algorithme de chiffrement à clé asymétrique. Le ransomware la chiffre avec la clé publique du serveur et l'envoie au serveur, qui déchiffre le message avec la clé privée associée à la clé publique utilisée dans le chiffrement, le serveur enregistre cette clé de session avec d'autres informations relatives au PC infecté (ID..).

La clé symétrique utilisée pour chiffrer les fichiers est, soit créée par le ransomware une fois exécuté et envoyée au serveur C&C (avec d'autres informations comme l'ID du PC infecté)

et ensuite supprimée du PC infecté, soit créée dans le serveur et envoyée par la suite au ransomware, d'où l'importance d'avoir une communication sécurisée entre le ransomware et le serveur distant.

Certains ransomwares utilisent une clé publique générée par le serveur pour chiffrer les fichiers , pour ces derniers le niveau de sécurité de la communication n'est pas très important pour recevoir la clé. La majorité des ransomwares n'utilisent pas une clé publique générée par le serveur pour chiffrer les fichiers, ils utilisent des clefs de chiffrement plus courtes de type AES par exemple et donc un canal sécurisé entre ces derniers et leurs serveurs est primordial.
Les protocoles les plus utilisés par les ransomwares, pour sécuriser les échanges, sont ceux qui se basent sur la cryptographie asymétrique RSA, Diffie-Hellman, Courbe elliptique..

2.6 La demande de rançon

2.6.1 L'évolution des modes de paiements

Un des facteurs important qui a contribué à la monté des ransomwares, est l'apparition de nouveaux outils de paiement, à l'instar des devises cryptographiques.
Avant les premières utilisation des Bitcoins comme monnaie de payement des rançons (fin 2013 avec Cryptolocker), les cybercriminels utilisaient des modes de transfert d'argent légitimes et semi-légitimes pour recevoir l'argent de leurs victimes ou s'échanger des fonds entre eux , par exemple des comptes bancaires dans des paradis fiscaux, ou des devises numériques comme *E-gold* et *Liberty Reserve*, certains demandaient à leurs victimes d'envoyer des sms surtaxés ou d'appeler un numéro premium comme rançon.
Le problème pour les hackers est que la confidentialité des transactions avec ces systèmes n'est pas garantie, et après un certain temps, ces systèmes sont tous tombés suite à une enquête judiciaire ou pour d'autres raisons et les opérateurs téléphoniques surveillaient de près les identités des propriétaires des comptes premiums et collaboraient avec les autorités pour contrer les hackers.

Mais les choses ont significativement changé avec l'apparitions des crypto-devises (Bitcoin en particulier) ce mode de paiement est totalement anonyme et stable, sa nature distribuée (pas d'autorité centrale) rend impossible à des organismes et aux états de tracer ou de bloquer les transactions.
Le tableau ci-dessous(fig5) montre l'évolution des modes de paiement employés par les développeurs des ransomwares au fil du temps.

Année	Les Ransomwares les plus répondus	Rançon
1989	PC Cyborg	190$ sur un compte Panama Offshor au Panama
2005	GPCode, PGPCoder, Krotten, archiveus Mayarchive	100-200$ avec e-gold ou Liberty Reserve
2006	GPCode.AG	100-200$ avec e-gold ou Liberty Reserve
2008	GPCode.AK,	100-200$ avec e-gold ou Liberty Reserve
2010	Fake Windows Activation	paiement par des appels surtaxés ou des virements bancaires
2010	Winlock	paiement par des SMS surtaxés(10$)
2012	Reveton (AKA Police Trojan),	100-200 par UKash, PaysAfecard ou moneypak
2013	Stampek kit, OS-x Specific,	300ds Moneypak
2013	Cryptolocker 1.0 et Cryptolocker 2.0	200-500$ MoneyPak, UKash, Cashu, bitcoin
2014	CTB-Locker(Aka Critroni)	seulement en BTC (0.5 bitcoin, environ 300$)
2014	SynoLocker	environ 0.6 bitcoin
2014	Torrent-Locker	seulement en Bitcoins (0.5 bitcoin, environ 300$)
2014	Cryptowall 2.0	550$ en bitcoin
2015	Cryptowall 3.0	entre 500$ et 1000$ uniquement en bitcoin
2016	Locky	Montant variable en bitcoin

Fig 5

2.6.2 Le Pire des Cas (Le paiement)

Une société dont la documentation fiscale, par exemple, est chiffrée juste avant la date limite des rendus des déclarations fiscales, n'a parfois pas le choix que de payer la rançon. Dans une entreprise, les Ingénieurs IT doivent prendre en compte cette éventualité, en mettant par exemple une somme (entre 300 et 500$) en Bitcoins dans un portefeuille géré par ces derniers, de plus, il doivent savoir comment faire des transaction en Bitcoins.

Scénario: Les étapes ci dessous

1) On se rend sur un site qui propose l'échange de l'argent contre des bitcoins et on créé un compte (par exemple avec https://www.bitcoinsuisse.ch/en/index/). Un *transactionID* (comme le montre la fig 6) sera généré pour identifier la transaction, cet *ID* est important

pour la suite.

Fig 6

2) Voir Fig 3 du sous-paragraphe: Comment sait-on qu'on est infecté. On clic sur *Next.*

3) On choisit Bitcoin comme mode de paiement ensuite *Next.*

4) On copie le *TransactionID* généré dans le point (1), dans le champ prévu à cet effet dans la fenêtre de paiement du CryptoLocker, comme le montre la Fig 7

Fig 7

5) On clique sur *Pay*, et on attend que le Ransomware vérifie le paiement et commence à déchiffrer les fichiers.

Attention:

- *Le paiement de la rançon dans les délais ne garantit pas à 100% la récupération des fichiers.*
- *Vous devrez reconnecter les disques externes/USB pour permettre au ransomware de les décrypter!*

CHAPITRE II
Mise en Oeuvre, Analyse et Monitoring d'un Ransomware

1. Méthodologie de travail

Avant de commencer ce rapport, j'ai analysé plusieurs ransomwares avant de trouver les rançonlogiciels à développer, je commencerai par analyser "Lorobot", dans la deuxième partie, j'analyserai "GpCode" pour mieux comprendre les Packers, et enfin "Locky".

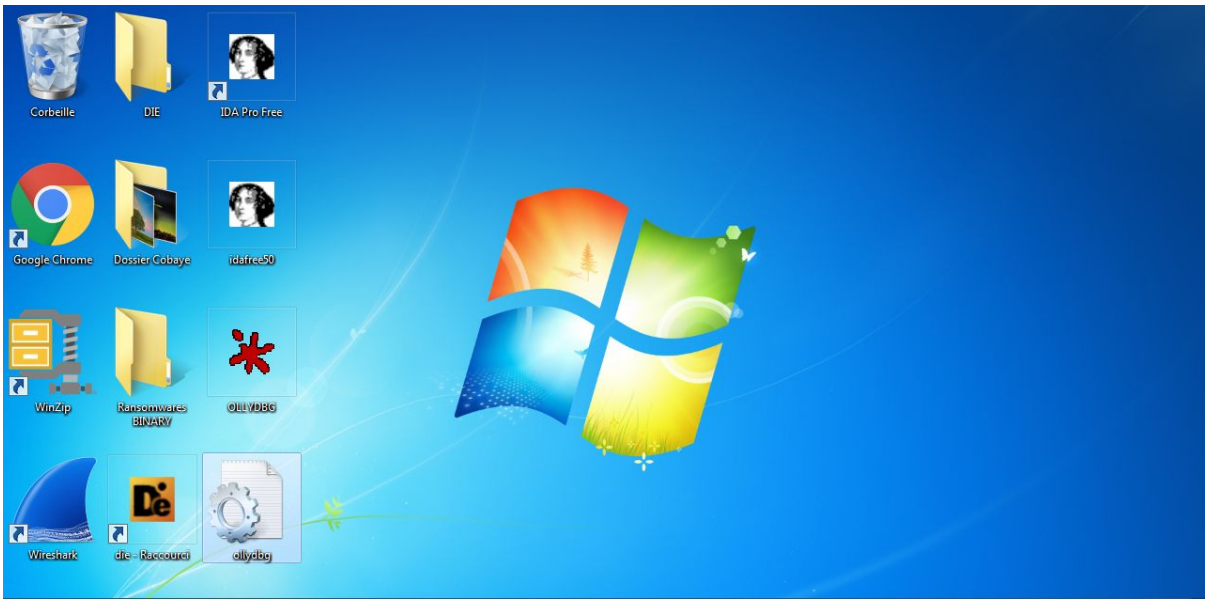
Mes sources sont fiables et variées, comme les laboratoires MalwareBaytes, Avaste, Kespersky.. avec leurs rapports, j'ai toujours essayé de garder une approche critique vis à vis des analyses. J'ai aussi vérifié que les sources étaient indépendantes entres elles (pas de source qui avait une autre analyse citée comme référence).

J'ai utilisé le site http://asm.inightmare.org/opcodelst/ pour comprendre les instructions Assembleur, j'utiliserai aussi l'annuaire des fonctions système microsoft (API) https://msdn.microsoft.com/en-us/library/windows/desktop/ms684847(v=vs.85).aspx pour comprendre le rôle des fonctions appelées par le binaire.

J'ai exécuté et analysé les ransomwares dans une VM et vérifié que la machine virtuelle ne partage aucun dossier avec la machine hôte. La quasi majorité des ransomwares sont packés (contiennent un packer qui compresse/chiffre le binaire) ce qui a rendu l'analyse plus dure.

J'ai crée plusieurs Snapshot de la VM avant l'exécution des ransomwares, et ce, pour éviter de tout réinstaller après chaque infection.
Les Samples (binaires) des ransomwares que j'ai téléchargés sont dans des fichiers ZIPs, avec un mot de passe (souvent infected, pour que le zip ne soit pas scanné et détruit par le Password AV). Quand on télécharge les binaires des ransomwares, ces derniers sont sans extension précise, donc on pourra les désassembler mais pas les exécuter, pour les exécuter il faut ajouter l'extension '.exe' aux binaires et ensuite les exécuter en tant qu'Administrateur pour les voir en action.

2. Environnement de Travail



1) Une machine Virtuelle: Windows 7, 64 bits, 3 Go.
2) Un “Dossier Cobaye”: contient des images qui seront chiffrées lors de l'exécution des Ransomwares.
3) Un dossier “Ransomwares BINARY”: Contient les binaires des ransomwares à étudier
4) Le Logiciel IDA Pro(version gratuite): Un désammeubleur statique.
5) Le Logiciel OLLYDBG: C’est un debugger qui exécute le malware pas à pas et nous permet de voir l’état des registres et de la Stack(Pile), on a aussi la possibilité de mettre des breakpoints.
6) Le logiciel DIE(Detect It Easy): pour détecter les Packers
7) WireShark.

3. Lorobot

Objectif: L'objectif principal de cette partie du rapport est de faire une analyse de la technique utilisée par ce ransomware (qui a fait son entrée en 2009 et est assez ancien par rapport à Locky, plus récent), en décortiquant les rôles joués par les fonctions et les codes contenus dans ses principaux blocs.

3.1 Le ransomware Lorobot

Lorobot est un ransomware qui a fait son apparition en 2009, j'ai choisi ce ransomware car il est relativement facile à comprendre et à désassembler, il ne contient pas de packer (ce qui est rare dans le monde des ransomwares), son code source est directement analysable après le désassemblage, son exécution est sequentielle (un seul processus et un seul thread).
De plus il ne teste pas s'il est en train d'être exécuté dans un environnement contrôlé, en outre à cette époque les ransomwares utilisaient des fonctions de chiffrements relativement simples comparées aux méthodes de chiffrement utilisées par les ransomwares actuels (on verra en détail la fonction de chiffrement de Lorobot).

3.2 Exécution de Lorobot

Avant tout, il faut ajouter l'extension ".exe" au binaire de Lorobot, ensuite, une fois Lorobot exécuté, le fond d'écran (wallpaper) change comme le montre la Fig 1, le wallpaper nous annonce:

- Qu'on vient de se faire infecter par un ransomware qui a chiffré nos fichiers avec un algorithme de chiffrement AES-256.
- Qu'il nous est impossible de restaurer nos fichiers sans la clé de déchiffrement.
- Qu'on doit prendre contact avec le ravisseur par email pour restaurer nos fichiers.
- Que la rançon s'élève à 100$, par exemple.

Les images contenues dans le "Dossier Cobaye" sont impossibles à ouvrir, de même pour les autres fichiers présents sur le disque (les fichiers textes sont désormais illisibles).

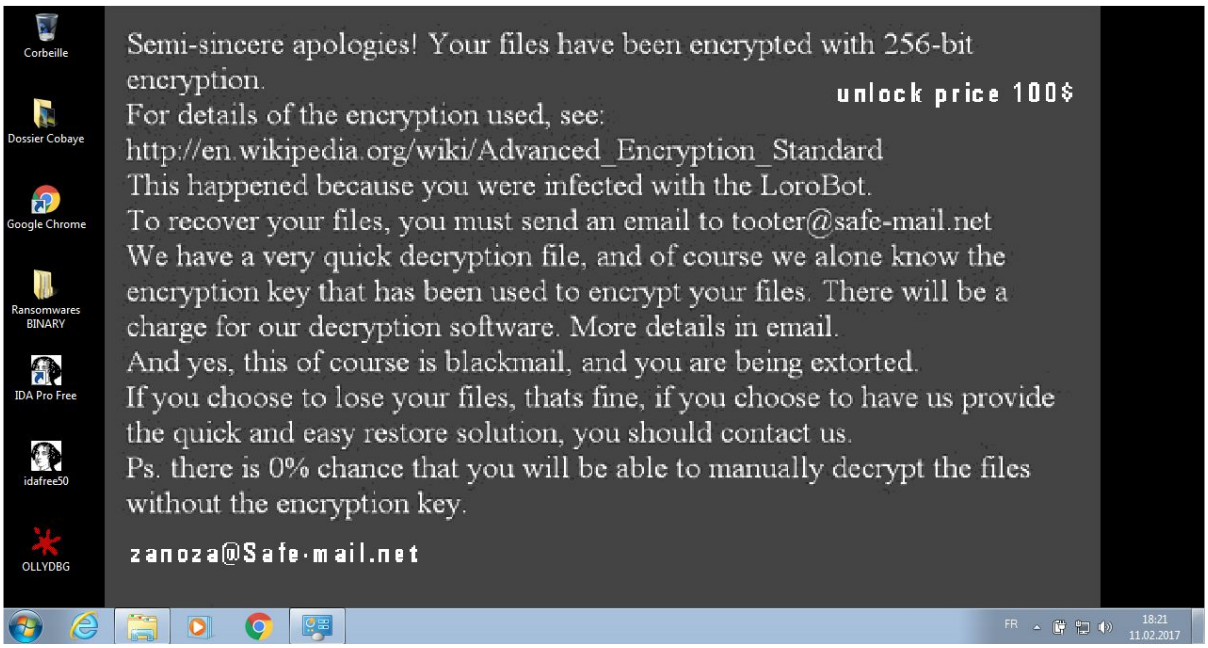


Fig1

3.3 Analyse de Lorobot

Dans cette partie, pour analyser Lorobot, je suivrai le schéma général d'une infection par ransomware présentée déjà dans la partie (I) du rapport.
Toute action exécutée par Lorobot, qui ne figure pas ou qui ne suit pas l'ordre chronologique des étapes du schéma de la figure C, sera mentionnée.

Figure C

3.3.1 L'infection

On lance IDA Pro (en mode Admin), et on importe le binaire de Lorobot, le code du binaire est représenté avec des blocs, qui peuvent être considérés comme des fonctions.

Dans le cas où il y a un test à la fin d'un bloc, si le test est "vrai", une flèche verte conduit vers un autre bloc, si le test est "faux", une fléche rouge nous conduira vers un autre bloc. Une flèche bleue est utilisée pour relier les blocs ; s'il n'y a pas de test ou pour représenter des boucles "For", une flèche verte peut aussi représenter une boucle "While".

Le premier bloc est le "Enty Point" du binaire, c'est l'équivalent de la fonction main() en C, le voici:

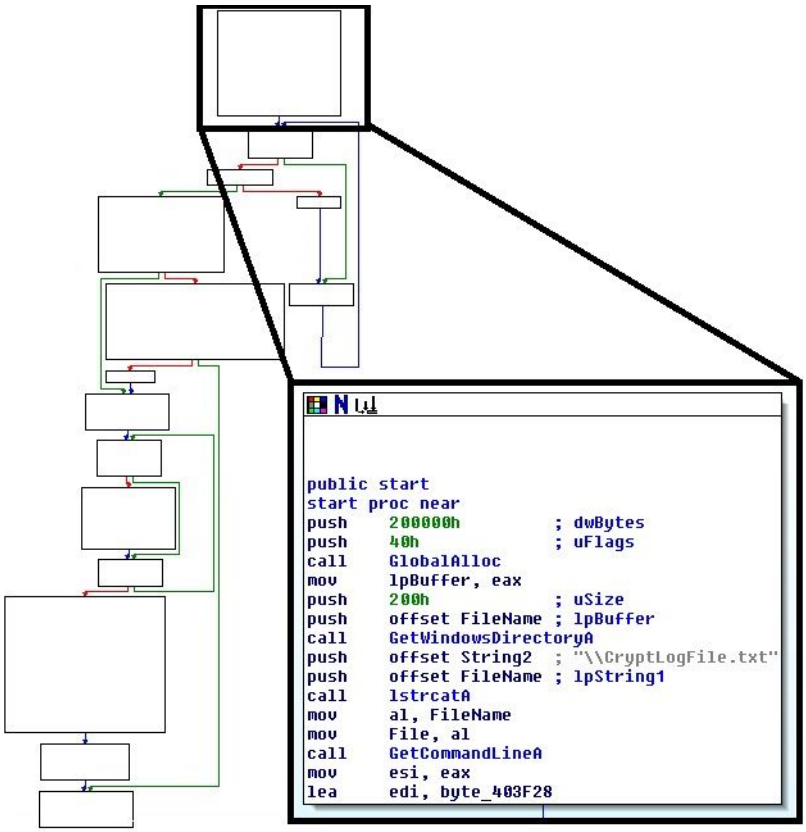


Fig2

Lorobot créé un fichier “CryptLogFile.txt”, ce fichier stockera les noms des fichiers que le malware a réussie à chiffrer.
Lorobot créé une image(qu’il extrait de son binaire) et met comme image de fond d’écran, cette image annonce à la victime qu’elle a subit une attaque par un ransomware.

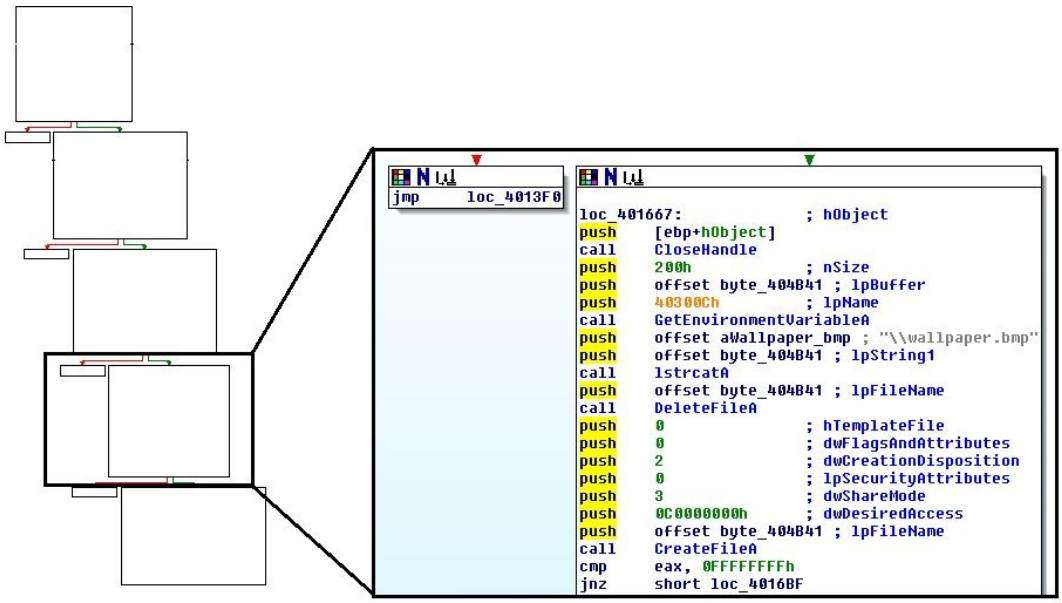


Fig 3

3.3.2 La diffusion

Lorobot utilise peu de méthodes pour se propager et infecter des machines, le mécanisme de propagation est simple, l'exécutable est attaché à des emails envoyés à des victimes, les emails prétendent être envoyés par des sites de réseaux sociaux populaires, de banques, ou des administrateurs informatiques, ils sont couramment utilisés pour attirer les victimes sans méfiance.

3.3.3 La communication

Lorobot ne communique pas directement avec un serveur en particulier ni avec son créateur pour recevoir l'ordre d'infecter un pc, c'est un ransomware automne. Après l'infection et le chiffrement des fichiers Lorobot laisse une adresse email que la victime doit à contacter pour récupérer ses fichiers.

3.3.4 La recherche des fichiers

Lorobot récupère les disques présents (C: D: ..), Fig 4, on remarque que Lorobot ne se limite pas à chiffrer le contenu du disque "C:".
Les disques collectés dans le code de la figure Fig 12 seront passés en argument à la fonction sub_401000, avec l'instruction call sub_401000.

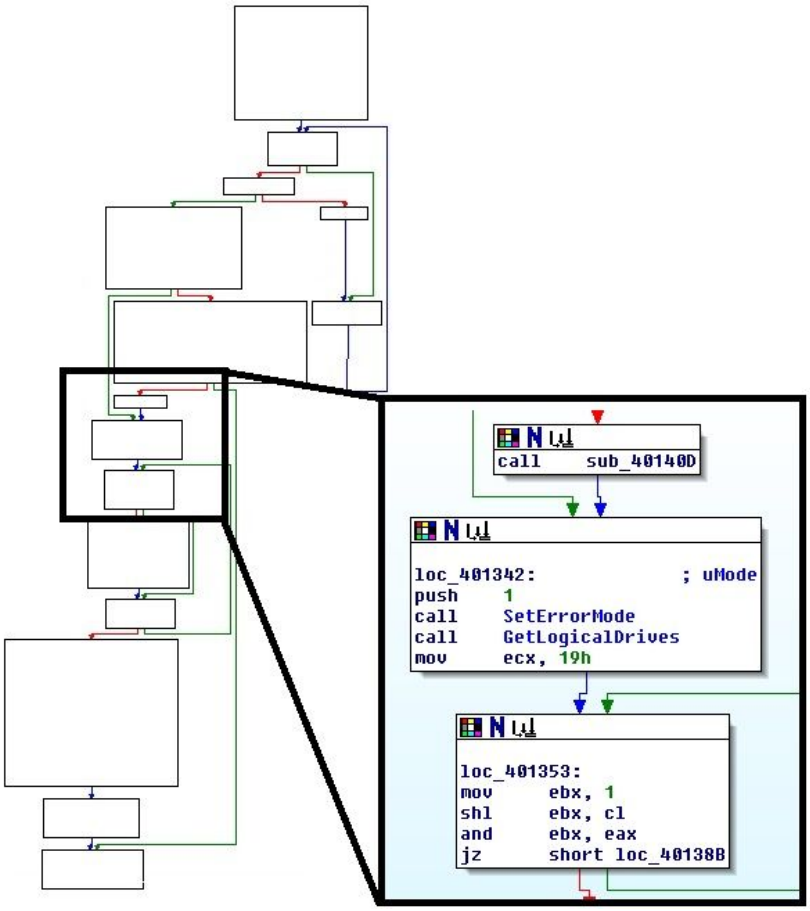


Fig 4

Pour chaque disque trouvé, Lorobot le parcourt et prend chaque fichier (avec la fonction FindFirstFile) et vérifie si l'extension de ce fichier figure dans la liste des extensions stocké dans la var a_doc_xlsdocx1(Fig 5), (si on double clique sur la variable a_doc_xlsdocx1 on voit les extensions que Lorobot chiffre) si elle y figure, il ouvre ce fichier, et le passe à la fonction de chiffrement.

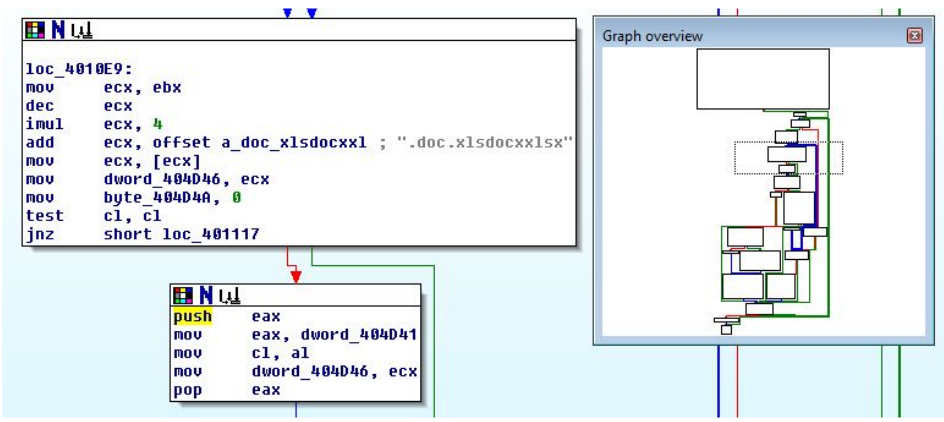


Fig 5

3.3.5 Le chiffrement

Lorobot prend la taille du fichier à chiffrer avec GetFileSize, l'ouvre une autre fois en lecture pour récupérer les données puis les passer dans une fonction de chiffrement et réécrit dans le même fichier les données chiffrées(par écrasement).
voici le code de la fonction de chiffrement(Fig 6).

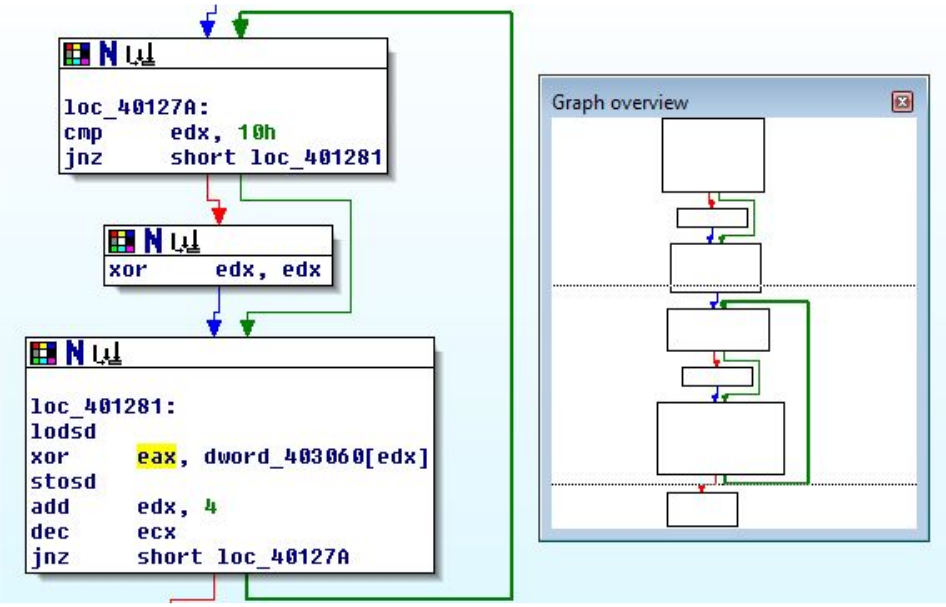


Fig 6

La boucle de chiffrement peut s'écrire ainsi en pseudo code :
Répéter{
fichier_cible[i] = fichier_cible[i] XOR clé[j mod 0x10]; i++; j++;
} Jusqu'à (fin de fichier).

Avec XOR si l'on chiffre un fichier avec une clé, on peut retrouver le fichier original et si l'on applique de nouveau XOR avec la même clé sur le fichier chiffré, à partir des données chiffrées et du binaire du ransomware on peut facilement déchiffrer les données.

Le développeur de Lorobot sait pertinemment que son ransomware utilise un XOR mais il essaye de tromper la victime et de lui faire croire que la méthode utilisée est le chiffrement AES-256 (méthode plus forte qu'un XOR), c'est une forme d'ingénierie sociale.

Lorobot ajoute les noms des fichiers chiffrés dans le fichier CryptLog.txt ("C:\Windows\CryptLogFile.txt") déjà rencontré au début de l'analyse, donc comme son nom l'indique c'est un fichier "Log", le software de déchiffrement que la victime recevra par email,

si elle paye la rançon, se basera sur ce fichier CryptLog.txt et sur la clé utilisée par le XOR pour déchiffrer les fichiers de la victime.

3.3.6 La demande de rançon

Une fois les fichiers chiffrés et leurs noms sauvegardés dans le fichier Log, ce code (Fig 7) permet de créer un fichier, d'écrire la phrase "Very bad news…" dedans, et de l'ouvrir en lecture pour informer la victime, c'est une façon très rudimentaire d'annoncer la mauvaise nouvelle à la victime, certains ransomwares actuels contineunt à utiliser les fichiers textes, sur les pages web qui s'ouvrent et qui expliquent en détail à la victime ce qu'elle doit faire pour récupérer ses fichiers.

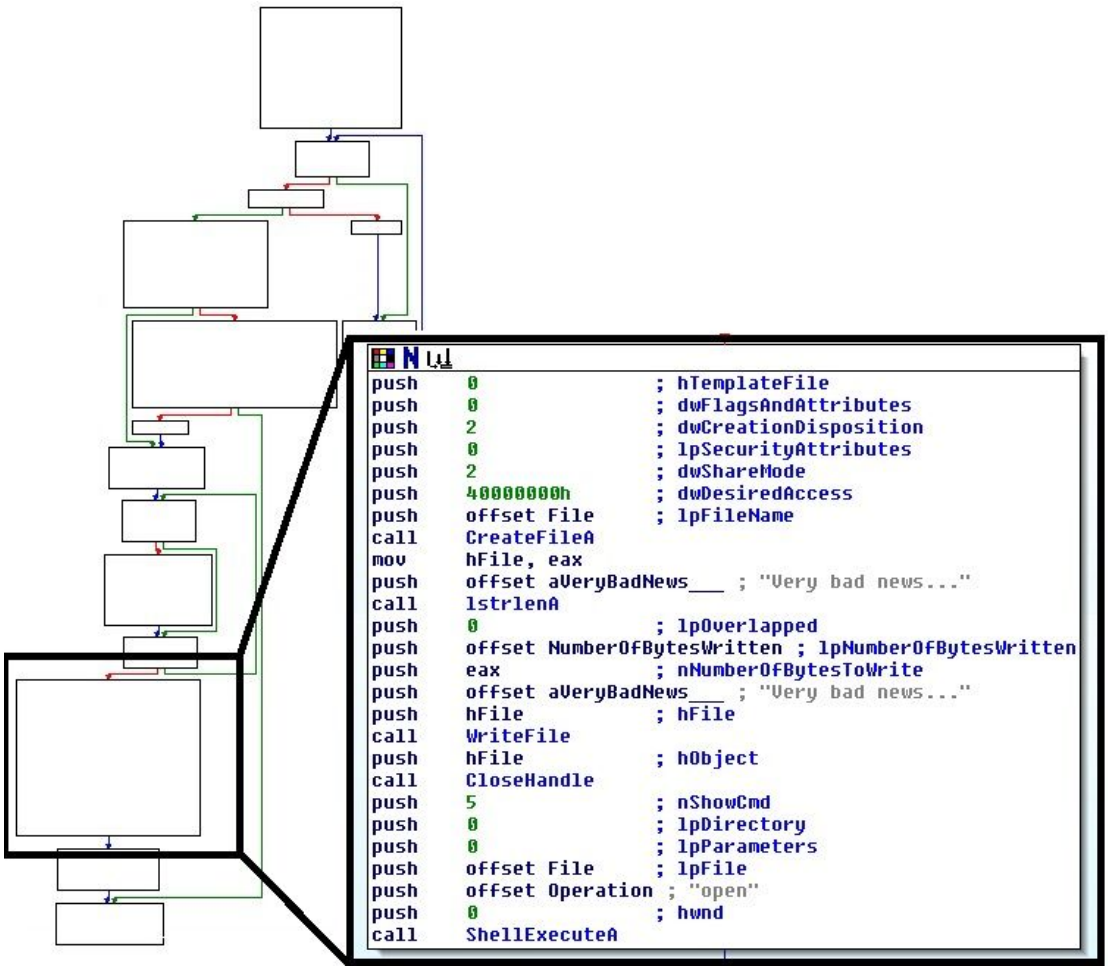


Fig 7

Liens:

Le binaire de Lorobot:
https://avcaesar.malware.lu/sample/d1a8c50ee845f68d1f95655dfe6e2ed99177676579f03bac39128352a5fba01a (il faut crée un compte pour le télécharger).

Assembleur x86:
https://fr.wikibooks.org/wiki/Programmation_Assembleur_x86
https://openclassrooms.com/courses/apprenez-a-programmer-en-assembleur-x86

4. Les Packers:

Objectif: Dans ce paragraphe je vais expliquer leur rôle protecteur de la charge utile d'un malware et la difficulté de les identifier par les scanners. Je présenterai, aussi, la méthode pour la décompression manuelle (en 9 étapes) du Packer UPX avec OLLYDBG.

4.1 Etude Théorique:

Lorsqu'on compile du code (C, Java..) vers le format exécutable de Windows('.exe') , selon le code utilisé, le fichier peut être volumineux.
Pour réduire la taille de ces fichiers executables, il existe ce que l'on appelle les Packers. Le packer permet d'empaqueter le fichier exécutable et de le compresser pour réduire sa taille. Au moment de l'exécution du fichier, le code du packer est appelé en premier pour décompresser le fichier exécutable avant qu'il ne soit exécuté.
Le malware 'packté' est similaire à un fichier 'zippé', sauf qu'on n'a pas besoin qu'un programme (Winzip, Winrar..) soit installé sur l'ordinateur pour décompresser le contenu, la routine de décompression est incluse dans le fichier compressé.

Les Packers tentent donc de contourner la détection des malwares par leurs signatures (par les Antivirus) et de ralentir le processus d'analyse des codes sources des malwares en se masquant comme un programme légitime.
Pour se masquer certains Packers ajoutent des métadonnées factices, une fois que le malware (Packer+Charge utile) est dans le système, le Packer décompresse la charge utile qui s'exécute et infecte le système.

Le rôle d'un Packer est essentiellement d'être la dernière et la plus complexe couche qui protégera la charge utile d'un malware. La figure P1 montre les couches de défense que le créateur d'un malware peut mettre en œuvre pour dissimuler la charge utile.

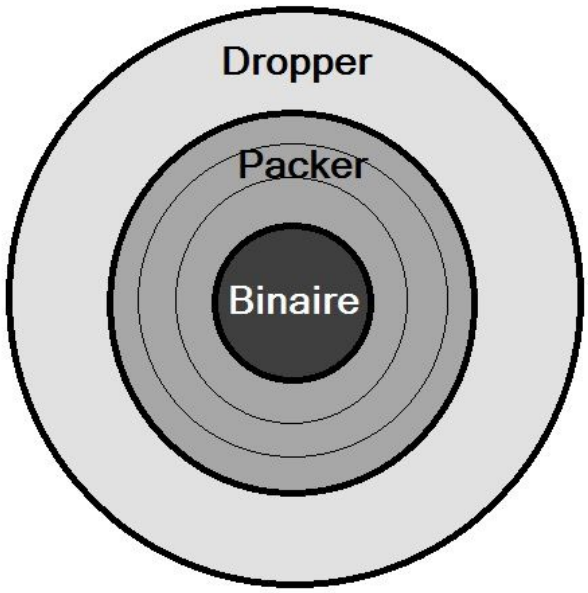


Fig P1

Dropper: c'est un injecteur quasiment identique au Cheval de troie, il a une apparence d'un fichier/programme légitime (e.g un Document Word pour Locky) mais permet de télécharger le Malware dans le système de la victime à son insu.
Packer: Un chiffreur/Compresseur, on peut déployer plus qu'un seul packer pour mieux protéger le Binaire.
Binaire: C'est la charge utile du Malware.

Généralement, les antivirus connaissent un certain nombre de Packers utilisés par des programmes légitimes ou par des Malwares, les antivirus sont constamment mis à jour dès qu'un nouveau Packer est identifié. Les exemples de packers connus: UPX, FSG…
Sauf que tous les jours, apparaissent de nouveaux packers méconnus des antivirus, lorsqu'un antivirus scanne un fichier dont le packer n'est pas connu, il ne sera pas en mesure de vérifier la signature réelle de ce fichier.
Les développeurs des malwares n'hésitent pas à empiler plusieurs Packers connus et moins connus pour protéger un code malveillant.

Mais il existe des packers plus complexes que d'autres, certains chiffrent ou compressent, et d'autres combinent compression et chiffrement, bien évidemment, les packers compresseur seront utilisés avant les packers chiffreur s'ils vont être utilisés ensemble(on compresse et après on chiffre, et non l'inverse).

Bien qu'il existe de nombreux programmes disponibles pour scanner les programmes ‘packtés’, il est impossible de les détecter tous, car de nouveaux packers plus sophistiqués sont régulièrement créés par des cybercriminels, ces packers ‘underground’ sont en vente sur des hangouts comme ‘Debug crypter’ ou ‘Cryptex’ et sur le deep web.

Cependant, les développeurs de malwares n’ont pas besoin d'un packer avancé pour tromper un scanner de fichiers(ou Antivirus). Parfois, ces scanners/antivirus peuvent être trompés en apportant de légères modifications aux packers préexistants.

4.2 Etude Pratique

J’ai choisi d’étudier le packer utilisé par la version 2010 de GpCode car la charge utile est protégée par un seul packer. J’utiliserai OllyDbg pour le “Unpakcing” du binaire de GpCode. En fonction du type et de la complexité du Packer, les opérations pour la décompression/déchiffrement peuvent varier en termes de temps et de difficulté, mais les opérations principales sont les mêmes: il faudra trouver la vraie Entry Point(OEP), faire un Dump du processus “unpackté” sur le disque et corriger de la table d'importation GpCode(2010) en action:

Fig P2

En ouvrant le binaire de GpCode dans IDA Pro, on remarque que GpCode est protégé contre le reverse engineering. on ne trouve pas les fonctions, les d’appels systèmes, les boucles.. mais juste une fenêtre qui nous donne des information utiles comme le nom du fichier.

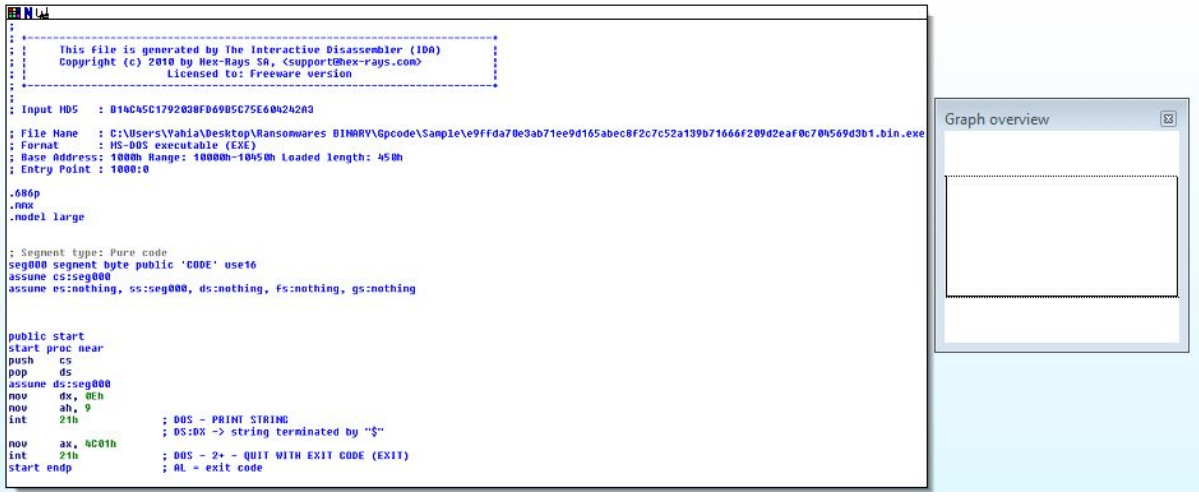


Fig P3(IDA Pro)

Avec OLLYDBG (Fig P4) on obtient pratiquement le même résultat, des lignes de code qui n'ont, à priori aucun sens.

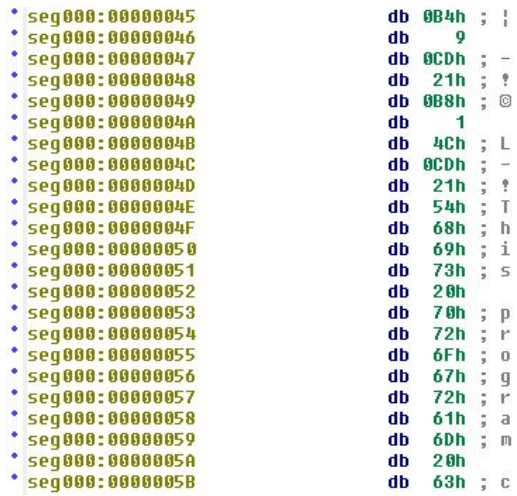


Fig P4(OllyDBG)

En premier lieu, il faudra scanner le binaire pour essayer de savoir quel type de Packer a été utilisé, seulement les packers usuels peuvent être identifiés, les packers customisés ou les nouveaux packers qui n'ont pas été identifiés ne seront pas reconnus par les scanners. "Detect it Easy" est un outil simple qui permet de scanner un binaire/exécutable, il est capable d'identifier un grand nombre de packers usuels que les développeurs de malwares utilisent, il fournit aussi d'autres informations concernant le binaire, tel que: le type de l'exécutable, la taille, le compilateur utilisé, le linker, l'entropie et plus..Il fournit aussi un éditeur Hexadécimal.

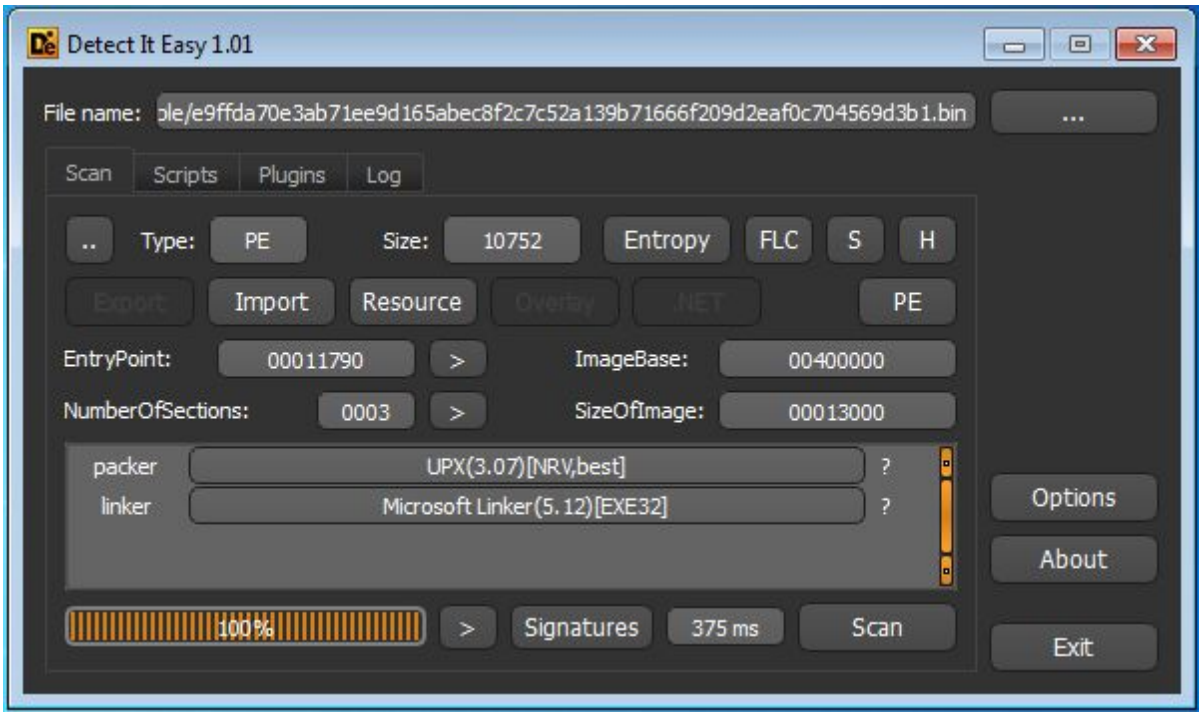


Fig P5

Detect It Easy, détecte le Packer : UPX(3.07), (Fig P5)
Je peux décompresser le binaire simplement avec la commande (upx -d GpCode), mais nous allons voir comment se passe réellement la décompression avec le debugger OLLYDBG, cette méthode permettra de décompresser beaucoup de Packers qui ont le même mécanisme de compression que UPX.

Les ransomwares actuels sont protégés par plusieurs packers en même temps, il suffira d'appliquer plusieurs fois le mécanismes de décompression("unpacking") et de vérifier à chaque fois si l'exécutable produit est "packé" ou non.

Commençons la décompression manuelle avec OllyDbg:

Etape 1:

On charge GpCode dans Ollydbg(l'exécuter avec les droits Admin):

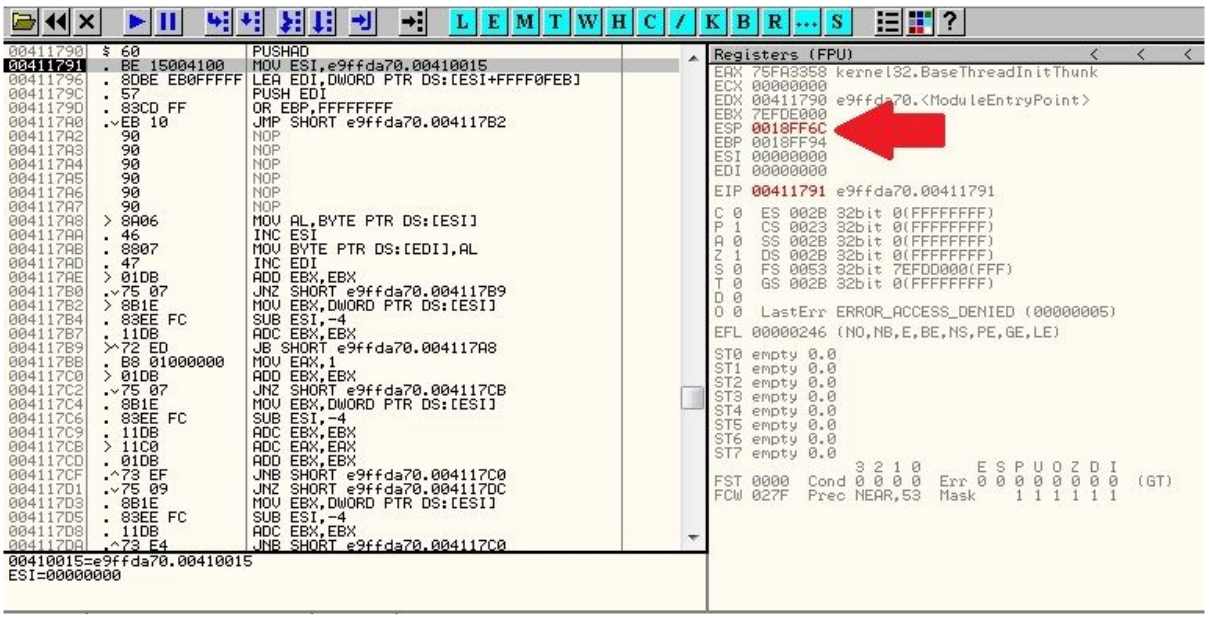


Fig P6

L'exécution s'arrête à l'instruction PUSHAD, on clique sur step into (F7), le curseur passe à l'instruction suivante (mov ESI, e9ffda70.00410015), on voit que la valeur du registre ESP a changé.

Etape 2:

Clic droit sur la valeur du registre ESP -> *Follow in Dump.*

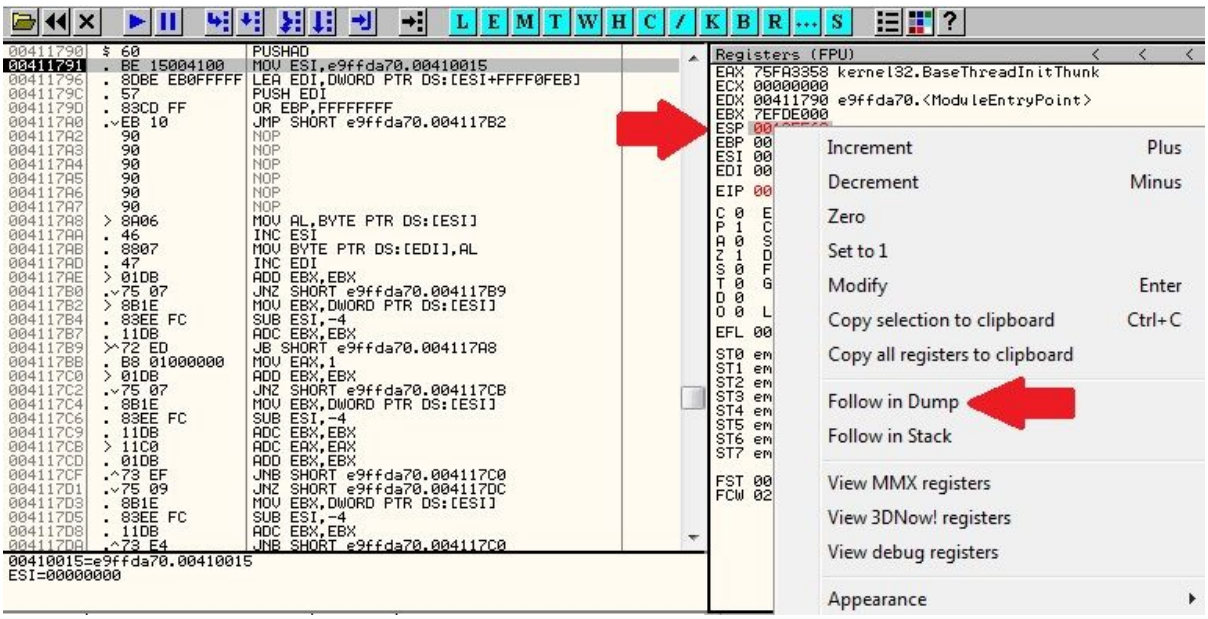


Fig P7

L’espace mémoire pointé par ESP est chargé alors dans la fenêtre Hex dump de Ollydbg, (voir Fig P8)

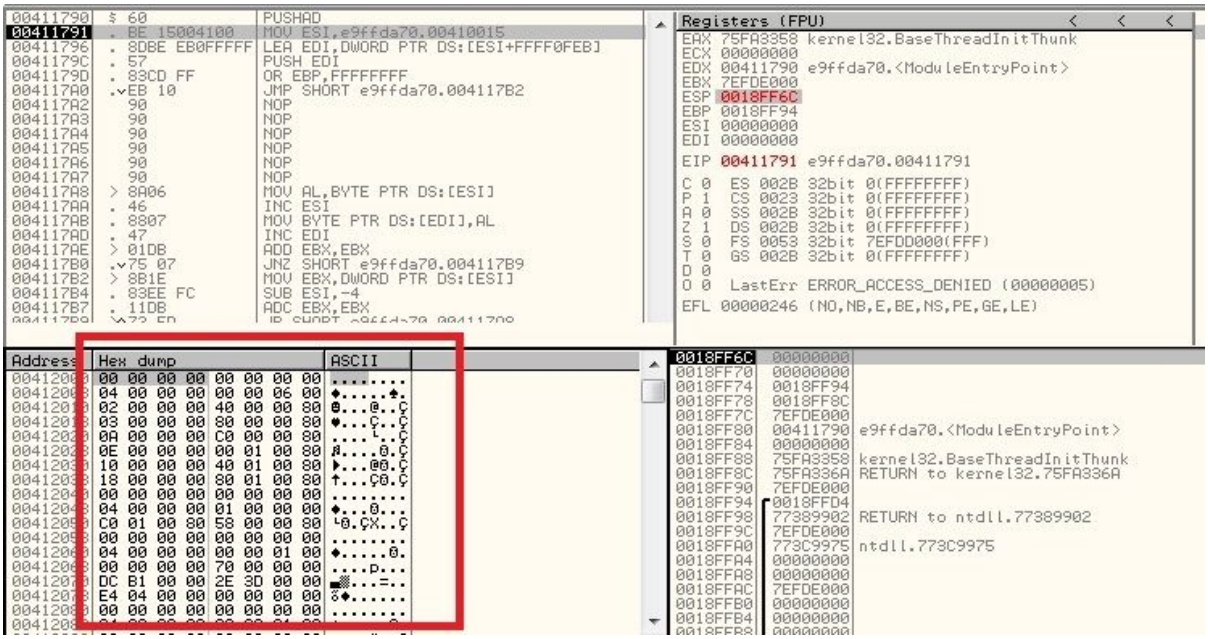


Fig P8

Etape 3:

On sélectionne les 4 premiers Bytes dans l’espace mémoire, clic droit, Breakpoint->Hardware, on access ->Word, ensuite on clique sur Run.

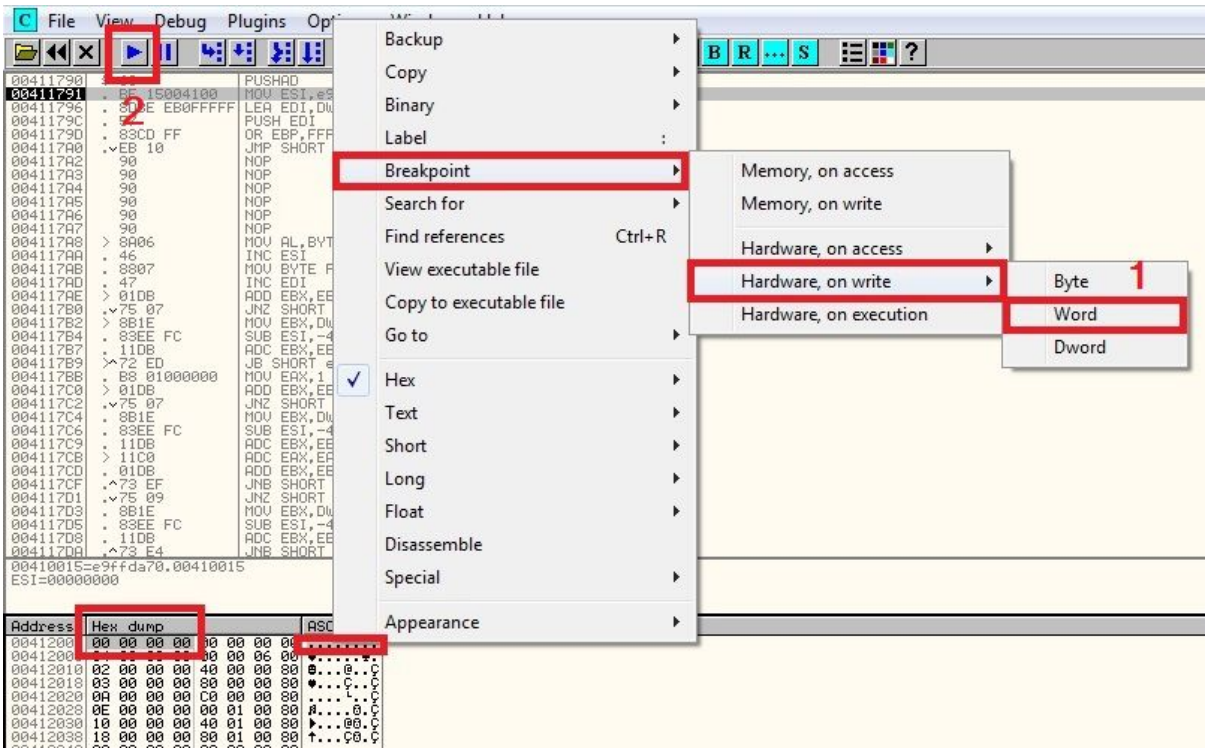


Fig P9

Etape 4:

Le debugger (Olly) saute à une autre partie du binaire, on ajoute un breakpoint à l'adresse de l'instruction précédent le JMP (sub ESP -80) cette instruction réserve un espace mémoire dans la pile pour décompresser le binaire original dans cet espace. On crée un breakpoint: breakpoint(1) -> Run(2), avec un Step over(3) et on est sur l'instruction JMP, on clique une deuxième fois sur step over pour exécuter l'instruction JMP.

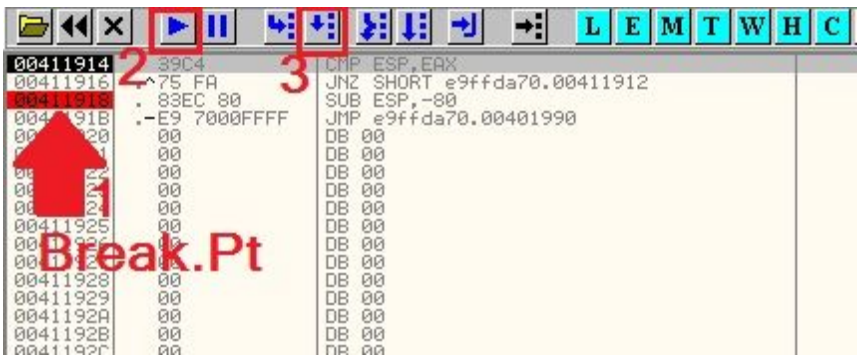


Fig P10

le JMP (saut) nous amène dans une partie du programme, nous somme au vrai Entry Point(EOP) du Programme. EOP=0x00401990.

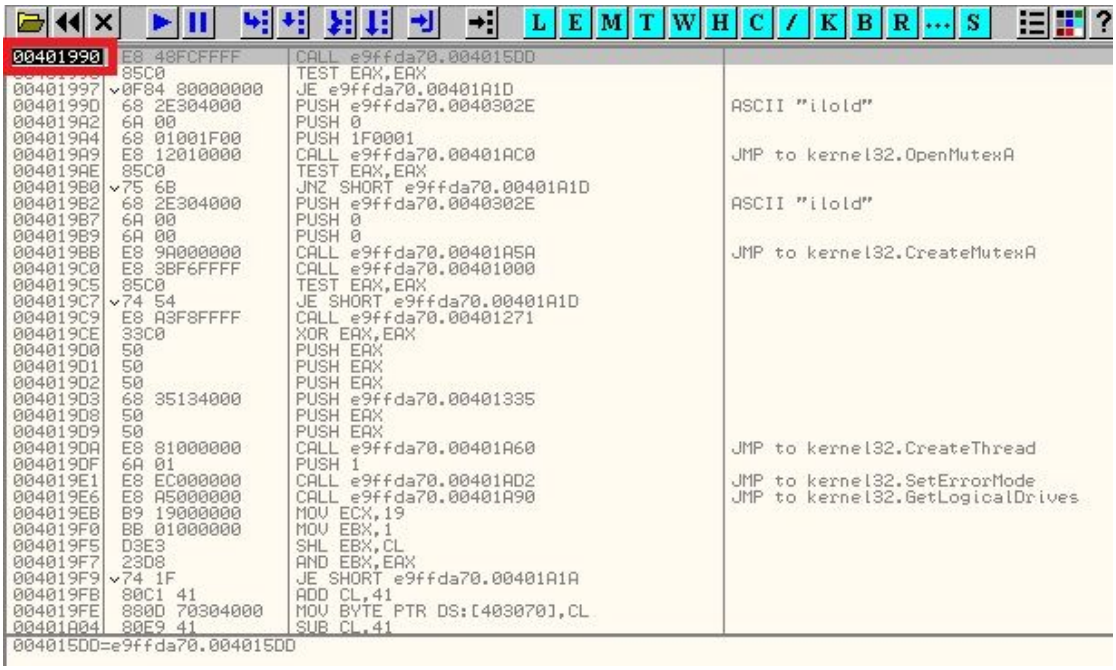


Fig P11

Etape 5:

Clic droit sur la première instruction-> Dump debugged process.

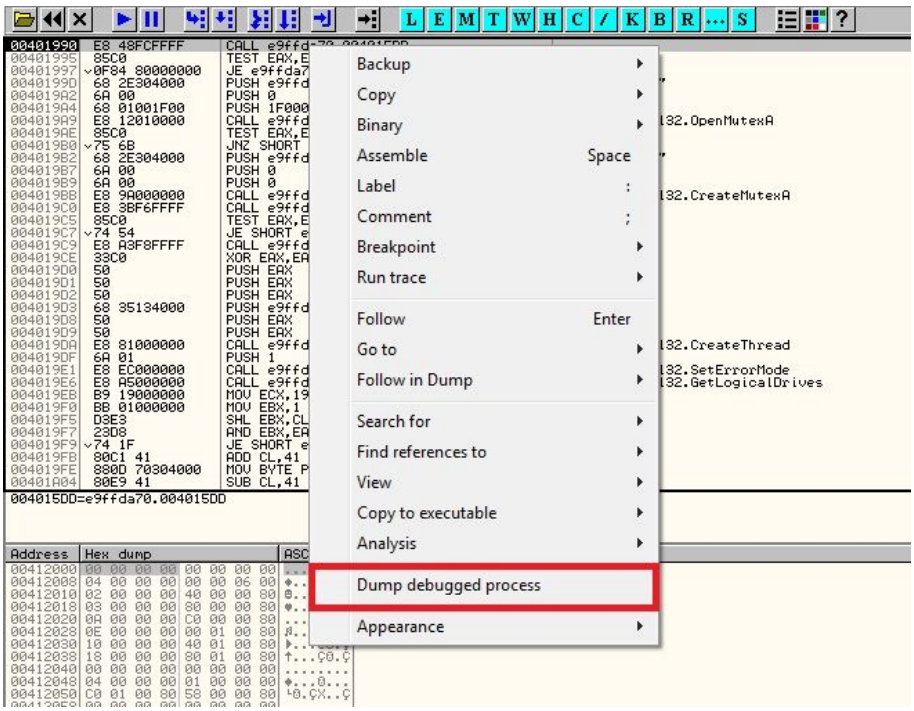


Fig P12

L’option “Dump debugged process” n’existe pas par défaut dans Olly, il faudra l’installer! A ce stade, le processus de GpCode est décompressé en mémoire, “Dump debugged process” décharge le processus débogué dans le disque.

Etape 6:

On obtient cette vu:

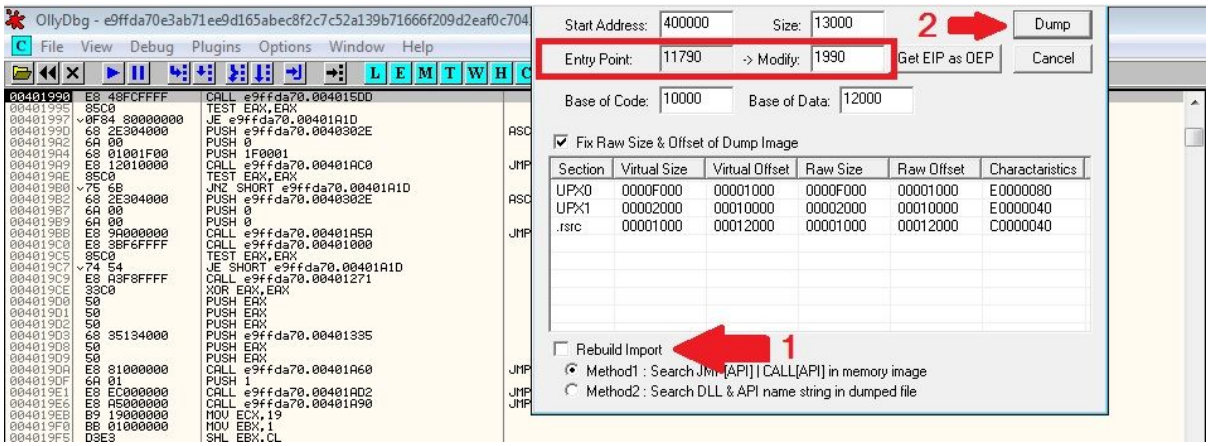


Fig P13

On décoche “Rebuild Import” car l'importation sera reconstituée en utilisant le logiciel (Import REConstructor) que nous verrons dans l’étape 8.
On distingue deux champs:
- Entry Point: C’est l’adresse de la routine de décompression de UPX - Modify: C’est l’adresse du vrai Entry Point de GpCode.
On note la valeur du champ “Modify”=(1990) pour la suite, et on clique sur Dump.

Etape 7:

On enregistre ces information “dumpé” dans un fichier GP_dump.

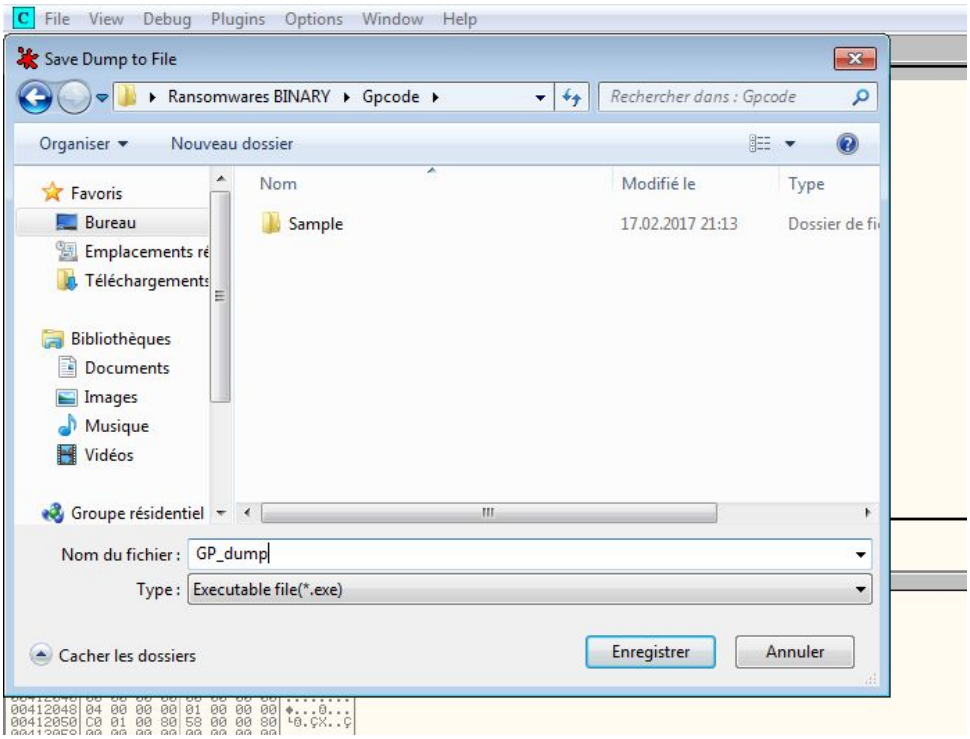


Fig P14

Le dump “GP-dump” ne s'exécute pas, il lui manque les “imports”.

Etape 8:

Laissons Olly de côté, et ouvrons le logiciel *Import Reconstructor*(ImportREC).

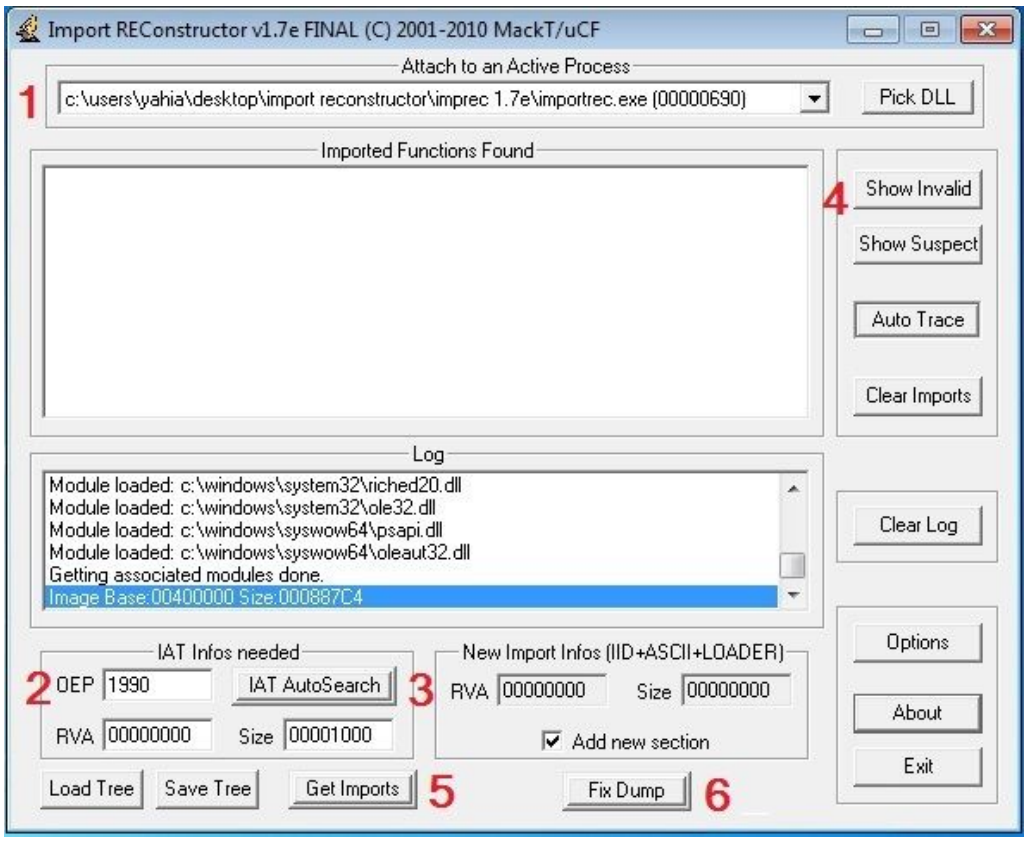


fig P15

2) Dans le champs “OEP”, on saisie la valeur de *Modify(1990)* qu’on a noté dans l'étape 6.
3) On clique sur “IAT AutoSearch” ensuite sur “OK”.
4) On clique sur “Show Invalid” pour voir s’il y a des erreurs.
5) On clique sur “Get Imports”.
6) On clique sur “Fix Dump”.

Une boîte de dialogue s’ouvre pour importer un fichier.

Etape 9:

On importe le fichier “GP_dump” créé à l’étape 7 avec Ollydbg.

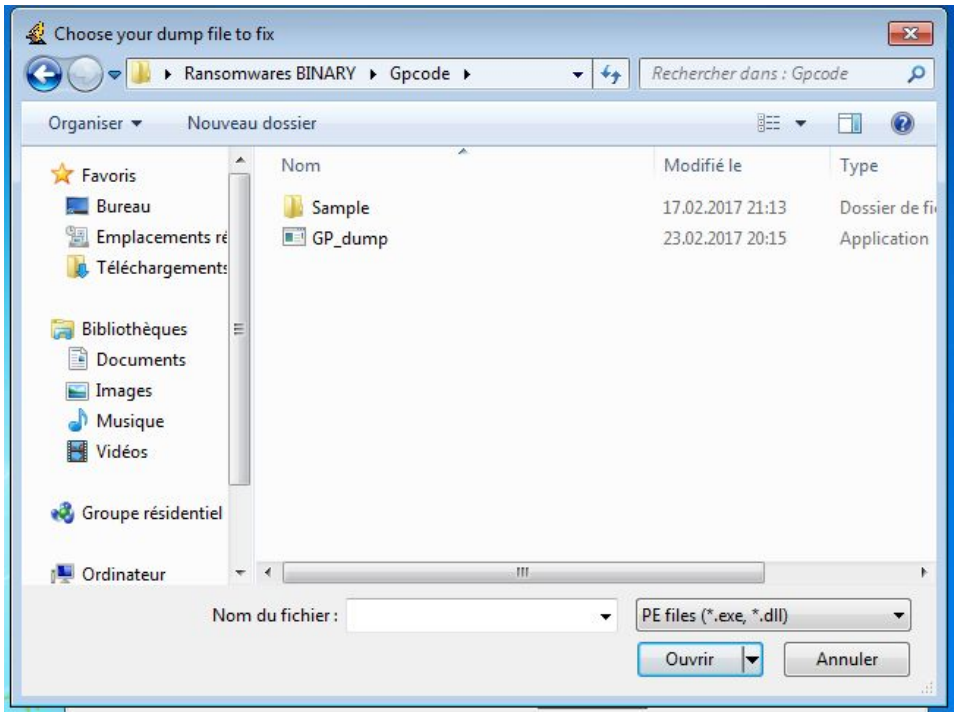


Fig P16

saved successfully: l'exécutable a été bien créé.

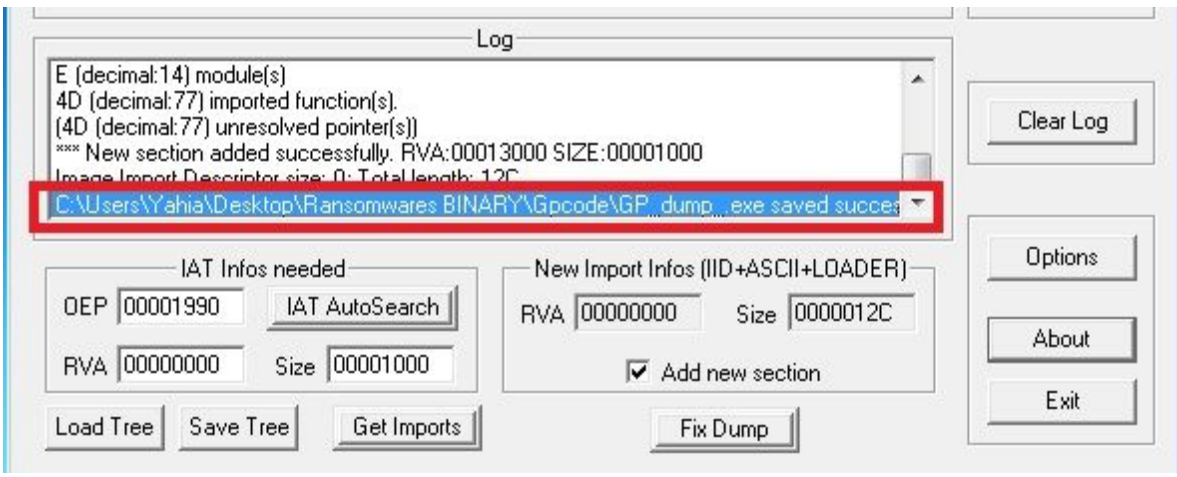


Fig P17

Un fichier exécutable “GP_dump_” est ajouté dans le même dossier que “GP_dump”.

Fig P18

On ouvre le fichier “GP_dump_” dans IDA Pro, l'exécutable est désassemblé correctement(Fig P19).

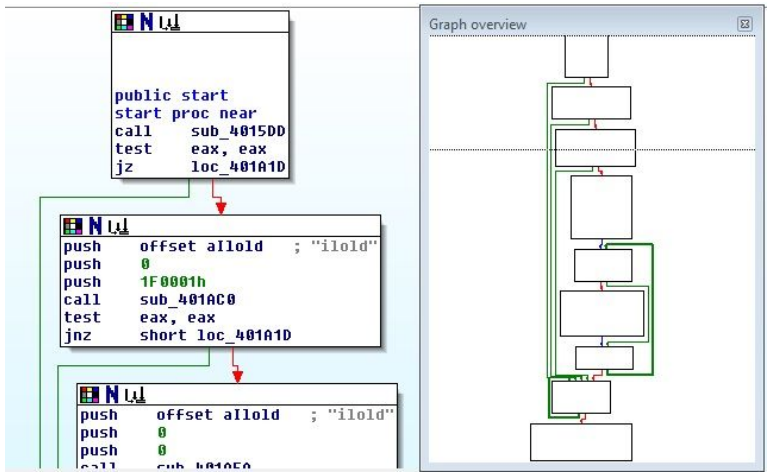


Fig P19

Une dernière vérification : si l’on ouvre “GP_dump_” dans DIE: On remarquera qu’il n’y a aucun Packer détecté!

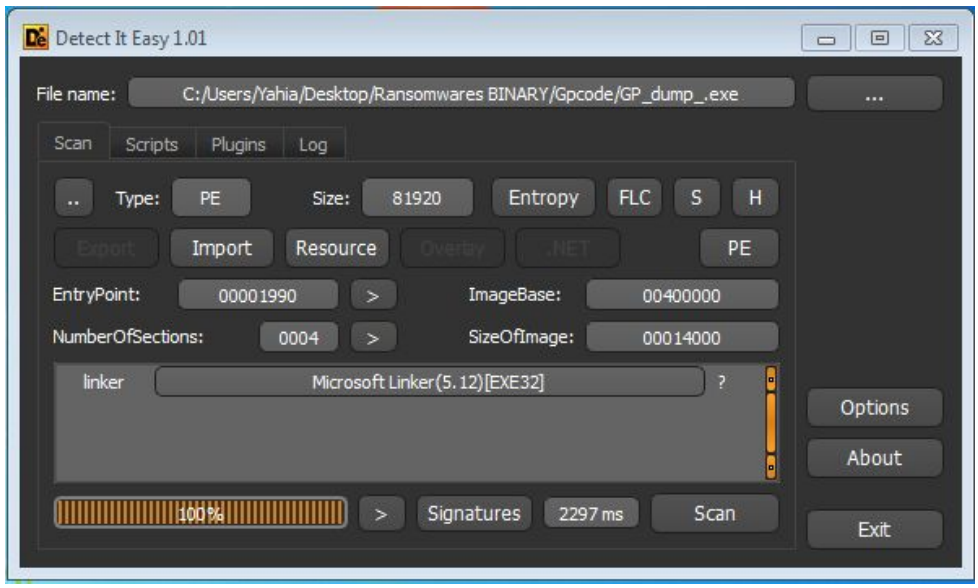


Fig 20

Liens Packer & GpCode:
http://securityxploded.com/unpackingupx.php
https://securityetalii.es/2012/12/03/a-very-light-introduction-to-packers/
https://blog.malwarebytes.com/threat-analysis/2015/12/malware-crypters-the-deceptive-first-layer/
How to PUT Plugin in OllyDbg: https://www.youtube.com/watch?v=6ytohtaOHHc&t=53s
http://support.kaspersky.com/us/1809

5. Locky

Objectif: J'analyserai, ici, ce ransomware récent (2016) pour les techniques intéressantes qu'il utilise et je décrirai les actions exécutées par lui, essentiellement en 6 étapes.

5.1 Le Ransomware Locky

Locky est apparue en février 2016, depuis l'année dernière il est l'un des ransomwares qui a le plus parler de lui.
J'ai choisi d'analyser Locky car il utilise des techniques intéressantes, certaines connues et d'autres propres à lui, tels que:

- Les DGA(Domain generation algorithms).
- Le chiffrement du canal de transmission.
- Le chiffrement hybride(RSA-2048 + AES-128).
- TOR / Bitcoins.
- Obfuscation de code et les Packers.
- Le chiffrement de plus que 160 types de fichiers(même les portefeuilles Bitcoins).
- Le chiffrement du contenue des disques virtuels et physiques.
- Une technique de diffusion particulière(qu'on verra par la suite).
- Une méthode de nommage des fichiers chiffrés particulière.

Le code source de Locky est plus complexe que celui de Lorobot, à titre indicatif, Locky est composé de plus qu'une cinquantaine de fonctions/blocs principales, contre une quinzaine pour Lorobot. La **Figure A** nous donne une vue globale des blocs du code source principale de Locky(comparé à celui de Lorobot). Les fonctions principales sont celles qui découlent

directement du main(), ces fonctions peuvent appeler d'autres fonctions, les schémas des codes sources sont en réalité plus complexe.

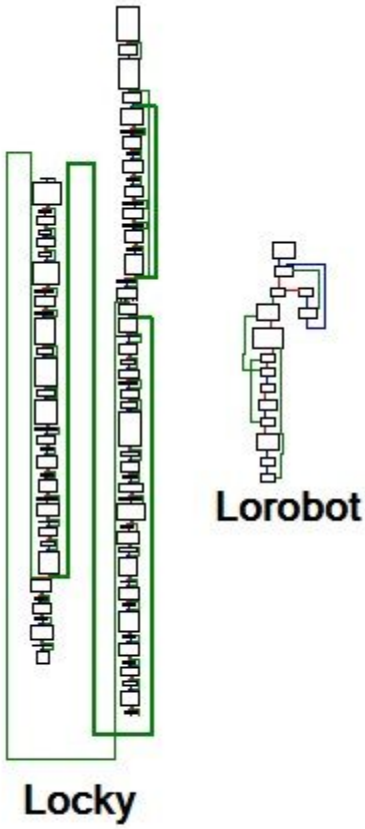


Figure A(avec IDA Pro**)**

Le but de cette analyse est de comprendre le fonctionnement globale du Ransomware Locky et non pas de l'analyser bloc par bloc. Seuls les blocs et les fonctions importantes seront analysés.

5.2 L'exécution de Locky

5.2.1 Obfuscation et Packer

La charge utile de Locky est bien protégée par des packers, la majorités des versions de Locky sont "packé" avec un packer customisé, des mécanismes semblables à ceux vu dans la partie Packer du rapport(Page 27) doivent être utilisés(il faudra entre autre chercher l'appel de

fonction *VirtualAlloc...*).
On commencera directement l'analyse de Locky, le packer utilisé ne sera pas analysé.

5.2.2 Exécution du binaire de Locky:

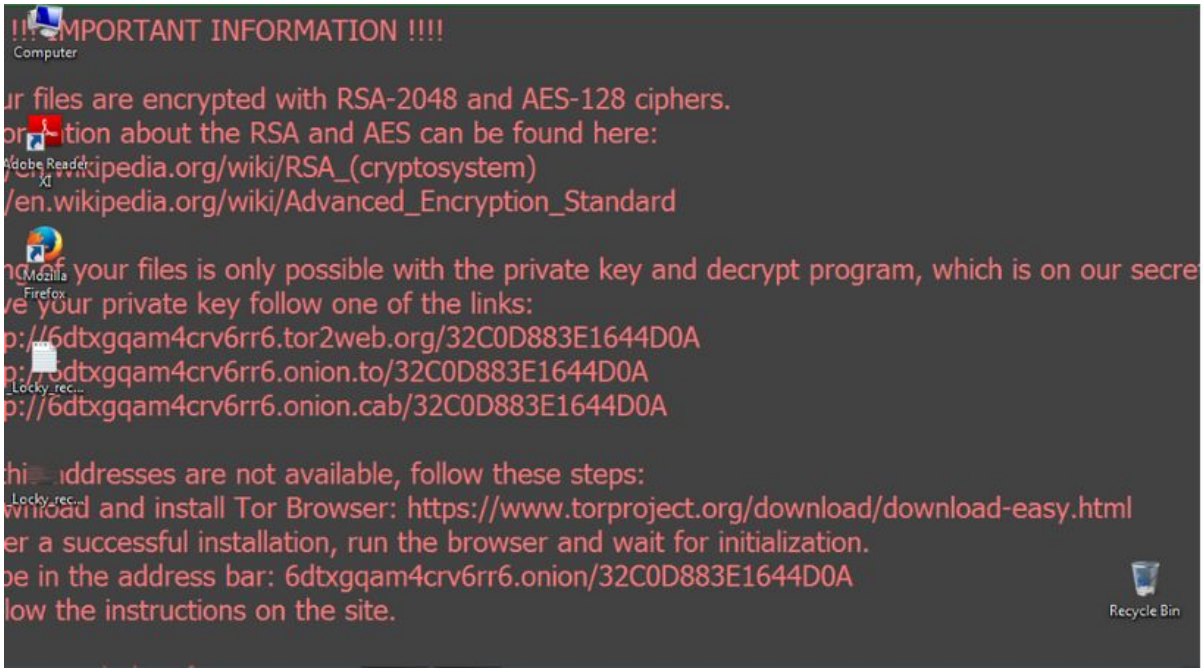


Figure B

Une fois une machine est infectée par Locky, le wallpaper change (Figure B), il nous annonce que nos fichiers sont chiffrés avec un algorithme de chiffrement fort (RSA&AES) et il nous explique ce qu'on doit faire pour les recuperer.
Le binaire de Locky contient des routines capables de détecter l'environnement de son exécution, si l'environnement est une machine virtuelle, le binaire malveillant ne s'exécute pas, et aucun fichier n'est chiffré, c'est une protection supplémentaire implémentée par les développeurs de Locky pour éviter que leur malware ne soit analysé.

5.3 L'analyse de Locky

Dans cette partie, pour analyser Locky, je suivrai le schéma général d'une infection par ransomware présentée déjà dans la partie (I) du rapport (Figure C).
Toute action exécutée par Locky, qui ne figure pas ou qui ne suit pas l'ordre chronologique des étapes du schéma de la figure C, sera mentionnée.

Figure C

5.3.1 La diffusion

Locky utilise plusieurs méthodes pour se propager et infecter des machines, mais le mécanisme de propagation le plus utilisé consiste à envoyer un courrier électronique avec un document malicieux de type Microsoft Word (.doc/.xls) en pièce jointe. Cette technique exploite une faille dans Microsoft Office.

Une fois téléchargé et ouvert, le document est illisible, un message d'erreur s'affiche expliquant à la victime qu'il doit activer les macros pour que le texte s'affiche correctement. Dans la Figure D on voit un exemple de document Word Malicieux.

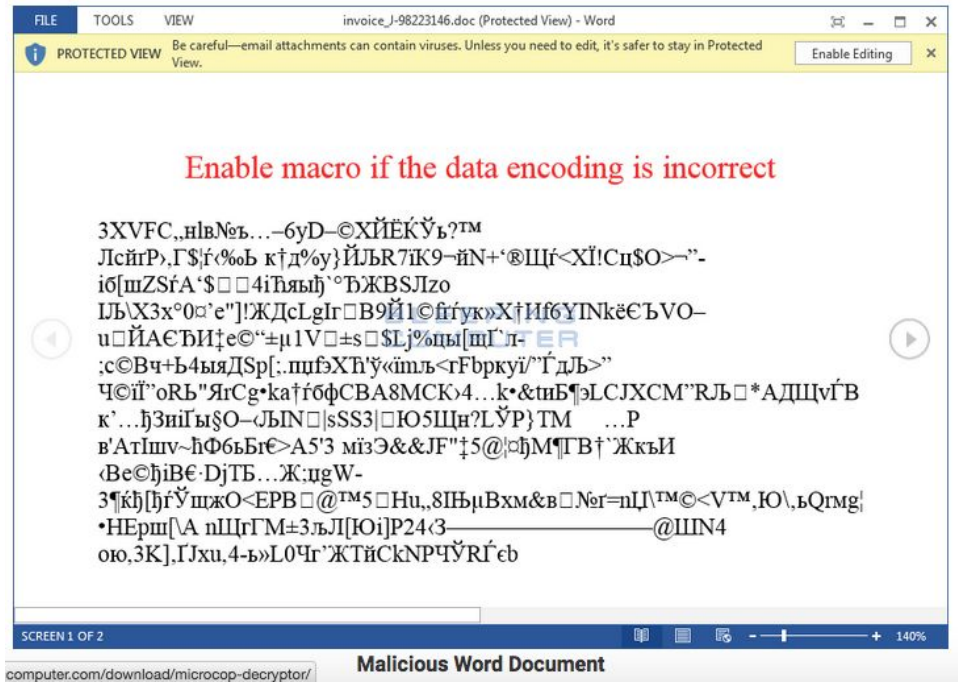


Figure D

L'activation des macros lance un script (le script est souvent écrit en VBA, un langage similaire à JavaScript). Les créateurs de Locky ont appliqué une méthode d' Obfuscation inhabituelle sur le script, via la fonction système CallByName appelée avec une chaine de caractère particulière.
Une fois déobfusqué, le script s'exécute, il lance le téléchargement du payload (charge utile) de Locky depuis un serveur distant. Dans le script, l'URL de téléchargement est codé en base64 et stocké "en dur" dans un tableau (KogdaGe7 dans la Figure C). Le script joue le rôle d'un cheval de Troie. Dans les dernières versions de Locky, une DLL chiffrée sera téléchargée au lieu d'un exécutable, cette DLL sera déchiffrée puis exécutée par l'outil de windows "rundll32.exe".

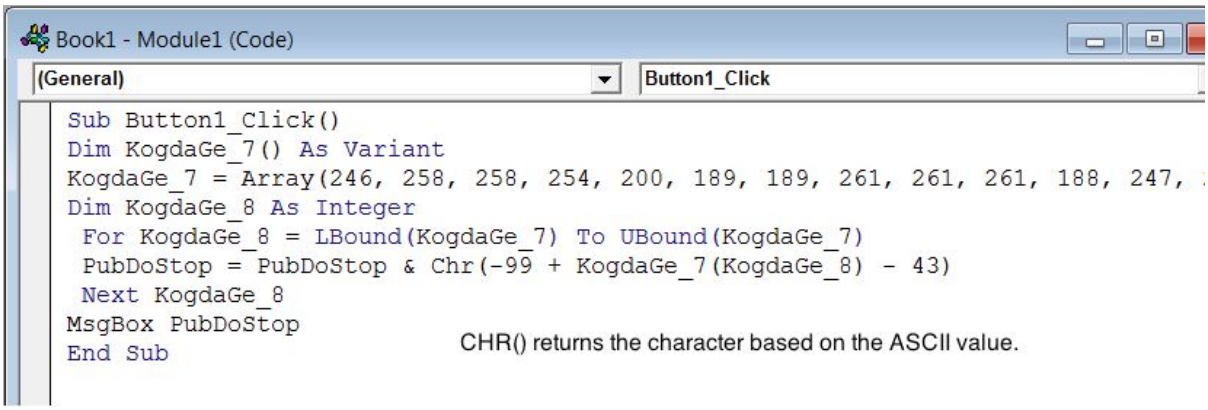


Figure E

5.3.2 L'infection

Une fois Locky téléchargé:

- Il stocke temporairement une copie de son binaire dans le dossier %Temp% (chemin complet C: \user\AppData\Local\Temp\svchost.exe), supprime le script(utilisé dans la diffusion), s'auto supprime, renomme sa copie en svchost.exe ou se donne un nom aléatoire(<random name>.exe / <random name>.dll) et s'exécute (à partir du dossier Temp).

- Il ajoute des clés dans la base de registre qui pointe sur son exécutable du dossier "Temp", pour pouvoir se lancer à chaque redémarrage du PC: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run"Locky" = "%TEMP%\<random name>.exe"

- Le nouveau processus Locky lancé depuis le dossier "Temp" commence par générer un ID unique pour le PC victime, pour celà, il fait appel à la fonction Get volume GUID, qui retourne le Path d'un Volume, ce path contient une chaîne alphanumérique (example: 2ev5a3z7-6g45-13f0-kjh6-965d6396f172) que windows génère de façon unique pour identifier un volume sur une machine, Locky génère le MD5 de cette chaîne, l'ID sera les 16 premiers caractères de cet Hash.

- Il supprime tous les fichiers VSS (Volume Snapshot Service) afin qu'ils ne puissent pas être utilisés pour restaurer les fichiers de la victime. Locky effectue cette opération en exécutant la commande : vssadmin.exe Delete Shadows /All /Quiet.

Une fois l'infection réussie et le chiffrement des fichiers est fait, le processus se supprime lui-même et supprime les clés qu'il a créées dans la base du registre.

5.3.3 La Communication

Locky effectue une série d'échange de paquets HTTP (POST) avec le serveur C&C, la "figure G" illustre une capture des paquets échangés entre la machine infectée et l'un des serveur C&C.

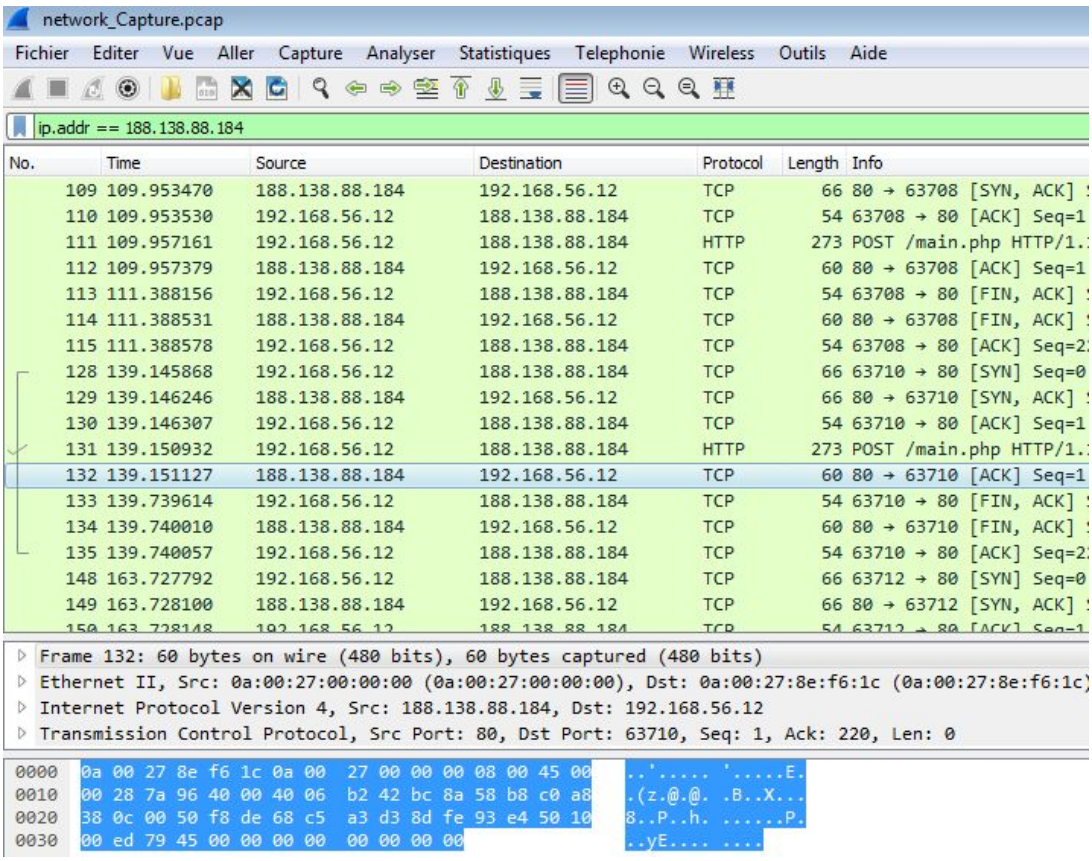


Figure G

On voit que la communication entre un serveur(188.138.88.184) et le PC victime (192.168.56.12) est basée sur les protocoles http (couche Application) et TCP (couche Transport). La communication est complètement chiffrée, vu que même les premiers paquets sont chiffrés, on peut deviner que la clé utilisée pour chiffrer la communication est contenue dans le binaire de Locky (chiffrement symétrique), cette clé n'a rien à voir, bien évidemment, avec la clé AES qui sera utilisée pour le chiffrement des fichiers.

Les adresses IP statiques des serveurs C&C sont codées en dur dans le code (ces serveurs se trouvent souvent en Russie, Ukraine..) comme le montre la Figure H, 31.41.41.37 / 188.138.88.184 / 86.25.138.167 sont les IPs des serveurs C&C.

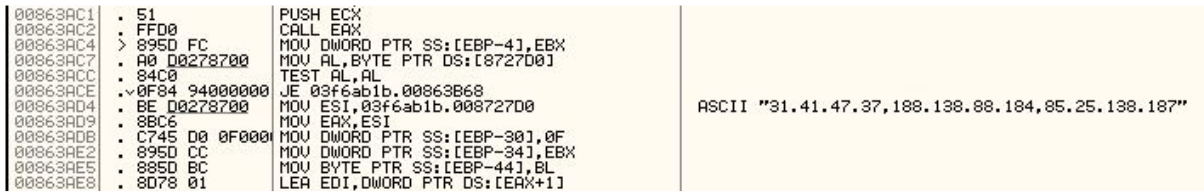


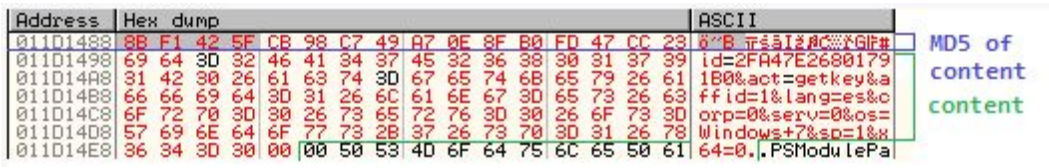
Figure H

De plus, Locky utilise les DGA (Domain Generation Algorithm), qui permettent de générer d'autres noms de domaines de façon sécurisée et anonyme, ces noms de domaines permettent aux hackers de garder le contrôle sur la machine infectée avec d'autres serveurs C&C en cas de problèmes avec les IPs statiques (s'ils seront bloqués par les ISP par exemple).
L''algorithme DGA implémenté dans Locky génère six domaines uniques tous les deux jours qui font office d'un point de rendez-vous entre la machine infectée et les serveurs C&C.

Le processus de Locky envoit et reçoit plusieurs informations pendant cet échange avec le serveur. Une clé de chiffrement(RSA-PubKey) est transférée du serveur au processus de Locky et stockée dans la variable 'pubkey' de la clé de registre 'HKCU \ Software \ Locky'.
(voir Figure I).
Entre autres, Locky envoie au serveur la langue utilisée dans le système infecté, l'identifiant unique ID qui a été généré localement dans le pc infecté, et des informations sur l'OS. Voici la structure des requêtes POST envoyées par Locky:

Requete POST:
id={personal_identifier}&act=getkey&affid={affiliate_id}&lang={language_code}&corp={is_enterprise_user}&serv={is_running_server_OS}&os={OS_name}&sp={servicepack_version}&x64={is_OS_64bit}
Requête POST:
id={personal_identifier}&act=gettext&lang={language_code}

Les Hahs(MD5) des requêtes POSTs sont calculés, ensuite le couple Requete/Hash(Requete) est chiffré et envoyé au serveur, qui fait de même, les Hashs assurent l'Intégrité des données échangées. Comme le montre cette capture:



La clé publique 'pubkey' ne sera pas utilisée pour chiffrer les fichiers, mais pour chiffrer les clés AES, ces clés(AES) seront utilisées pour chiffrer les fichiers du PC infecté. La clé publique servira aussi à chiffrer d'autres informations (fichiers Logs) que Locky enverra au serveur, nous verrons ce point en détail dans le point 5: Le Chiffrement.

Locky stocke les informations récoltées pendant l'échange avec le serveur et d'autres générées localement dans la base de registre sous les clés suivantes:
HKCU\Software\Locky\id : ID unique pour identifier la victime.
HKCU\Software\Locky\pubkey : La clé publique (RSA-2048) reçu par le serveur.
HKCU\Software\Locky\paytext : Le texte qui sera affiché dans le wallpaper.
HKCU\Software\Locky\completed : mis à '1' si Locy a fini de chiffrer tous les fichiers.

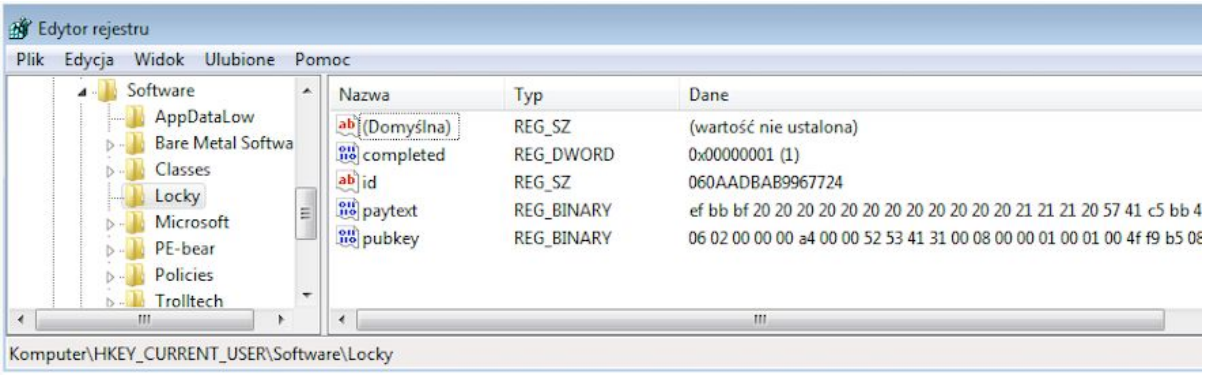


Figure I

Il est important de mentionner que Locky produit un wallpaper.bmp. et change l'arrière plan du pc dès le début de la communication avec le serveur C&C , donc le wallpaper est produit avant même l'exécution des étapes "Recherche des Fichiers" et "Chiffrement". Ce point sera détaillé dans le point 6: La Demande de Rançon.

Attention: En produisant un wallpaper.bmp avant l'exécution des étapes "Recherche des Fichiers" et "Chiffrement, Locky ne suit pas l'ordre chronologique des étapes du schéma de la figure C.

5.3.4 La recherche des fichiers

Dans cette portion de code (Figure J), la fonction système GetDriveType retourne le type de mémoire(dont lpRootPathName est le chemin), le processus boucle sur cette portion de code et pour chaque disque trouvé il cree un thread qui se charge de chiffrer le contenu du disque avec call run_encryption_thread. Locky cible 3 types de disques:

- Les Disques durs(C: D: ..) ou SSD..
- Les Disques externes(USB, Disque dur externe..).
- Les RamDisk(mémoire vive simulée en disque dur).

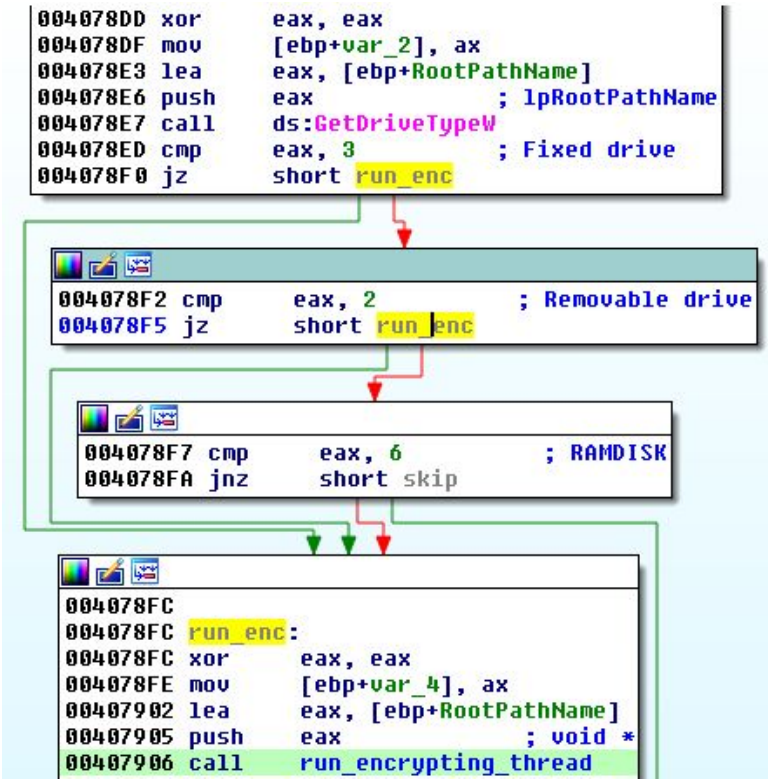


Figure J

Locky cible aussi les ressources partagées en réseau (même s'ils ne sont pas mappées sur un lecteur local (pour plus d'informations voir la Partie III: La Prévention,), ces ressources sont collectées à l'aide de l'appel système WNetAddConnection2 comme le montre la Fig K. Les données ainsi collectées seront listées et traitées par des threads chiffreurs comme avec les autres fichiers.

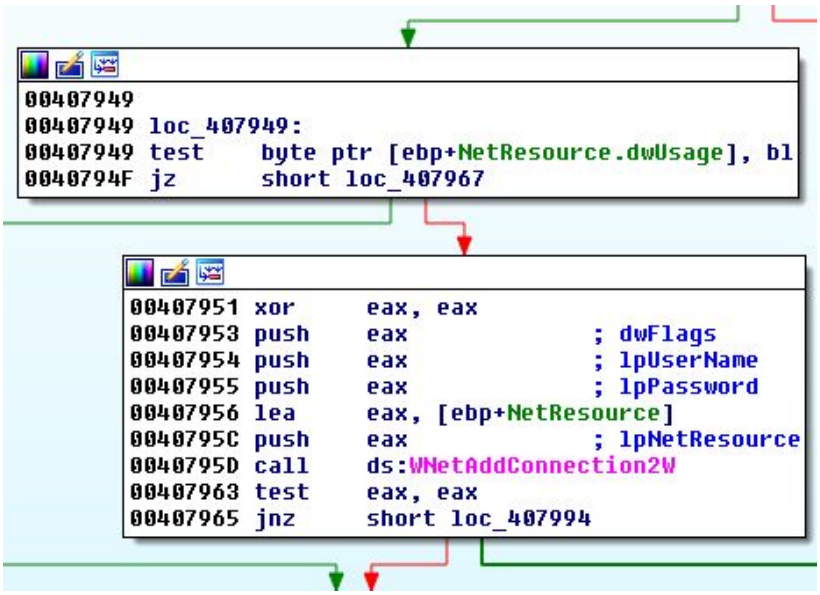


Figure K

Locky ignore tous les fichiers dont le chemin complet et le nom de fichier contiennent l'une des chaînes suivantes:

"tmp, winnt, Application Data, AppData, Program Files (x86), Program Files, temp, thumbs.db, $Recycle.Bin, System Volume Information, Boot, Windows".

Les créateurs de Locky ont évité d'endommager les fichiers essentiels au bon fonctionnement du système d'exploitation Windows, on voit que Locky épargne aussi les fichiers temporaires, c'est peut être aussi par souci d'efficacité, probablement ces créateurs ont voulu que Locky se concentre à chiffrer les fichiers les plus importants aux yeux d'un utilisateur comme les vidéos, les images..et même son portefeuille Bitcoin(Wallet.dat)! voici une liste non exhaustive des types de fichier visés:

".mid, .wma, .flv, .mkv, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .qcow2, .vdi, .vmdk, .vmx, .gpg, .aes, .ARC, .PAQ, .tar.bz2, .tbk, .bak, .tar, .tgz, .rar, .zip, .djv, .djvu, .svg, .bmp, .png, .gif, .raw, .cgm, .jpeg, .jpg, .tif, .tiff, .NEF, .psd, .cmd, .bat, .class, .jar, .java, .asp, .brd, .sch, .dch, .dip, .vbs, .asm, .pas, .cpp, .php, .ldf, .mdf, .ibd, .MYI, .MYD, .frm, .odb, .dbf, .mdb, .sql, .SQLITEDB, .SQLITE3, .asc, .lay6, .lay, .ms11 (Security copy), .sldm, .sldx, .ppsm, .ppsx, .ppam, .docb, .mml, .sxm, .otg, .odg, .uop, .potx, .potm, .pptx, .pptm, .std, .sxd, .pot, .pps, .sti, .sxi, .otp, .odp, .wks, .xltx, .xltm, .xlsx, .xlsm, .xlsb, .slk, .xlw, .xlt, .xlm, .xlc, .dif, .stc, .sxc, .ots, .ods, .hwp, .dotm, .dotx, .docm, .docx, .DOT, .max, .xml, .txt, .CSV, .uot, .RTF, .pdf, .XLS, .PPT, .stw, .sxw, .ott, .odt, .DOC, .pem, .csr, .crt, .key, wallet.dat..."**

Locky ne peut pas chiffrer les dossiers partagés "Hidden shares", voir plus d'informations sur les hidden shares dans la partie III: Prévention.

5.3.5 Le Chiffrement

Comme l'annonce le wallpaper, Locky utilise effectivement les algorithmes RSA et AES, le chiffrement est implémenté à l'aide de la librairie CryptoAPI de Window.
En premier lieu, le serveur génère une paire de clés avec l'algo RSA-2048 bits, la clé publique est envoyée à la victime, la clé privée reste dans le serveur.
Locky utilise ensuite cette clé publique pour chiffrer les clés AES, une clé AES différente des autres est générée aléatoirement pour chaque fichier à chiffrer.

Comme le montre le instructions de la figure L, pour générer ces clés AES, Locky fait appel à la fonction système CryptGenRandom et lui passe la valeur 16 (16 bytes = 128 bits) comme argument pour la longueur de la clé à générer (*push 16 ; dwlen).*

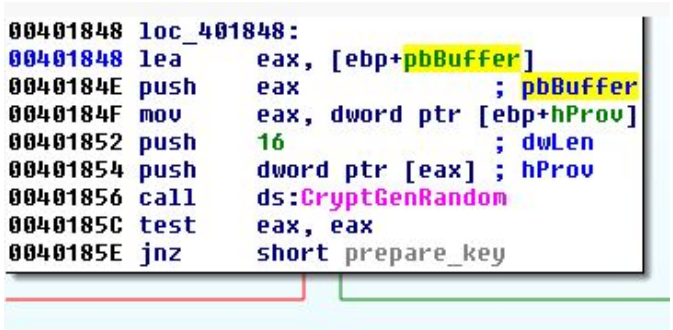


Figure L

Les fichiers collectés pendant l'étape "Recherche des Fichiers", sont regroupés dans des listes, des threads sont créés, chaque thread commence à chiffrer les fichiers avec des clés particulières utilisant l'algorithme de chiffrement AES-ECB(128bits).

Après le chiffrement, Locky renomme les fichiers. Les noms des fichiers sont comme suit: ([unique_id] [identificateur] .locky), unique_id est le même pour tous les fichiers du pc, c'est aussi l'identificateur du PC auprès du serveur, la valeur de l'ID est stockée dans la variable 'id' de la clé de registre 'HKCU \ Software \ Locky' , identificateur est généré aléatoirement, tous les fichiers ont une extension .locky(voir Figure M)

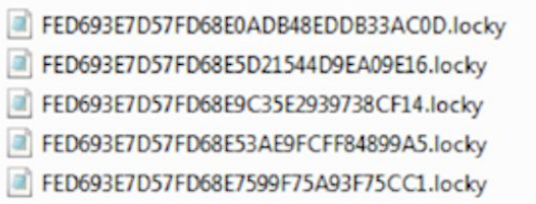


Figure M

Les instructions présentes dans chaque Thread de chiffrement (Figure N), nous montrent que les informations concernant ces fichiers chiffrés, ces Métadonnées comme l'ancien nom, le nouveau nom, les chemin et la taille sont collectés dans des fichiers Logs , ces fichiers Logs seront chiffrés (avec la clé publique) et envoyés au serveur C&C.

```
00402A82 mov     edi, eax
00402A84 lea     eax, [ebp+var_C8]
00402A8A push    offset aId_0    ; "id="
00402A8F push    eax
00402A90 mov     ebx, offset dword_416C78
00402A95 mov     byte ptr [ebp+var_4], 0Bh
00402A99 call    sub_404430
00402A9E push    offset aActStatsPath ; "&act=stats&path="
00402AA3 push    eax
00402AA4 lea     eax, [ebp+var_1C4]
00402AAA mov     byte ptr [ebp+var_4], 0Ch
00402AAE call    sub_4044AA
00402AB3 mov     ecx, eax
00402AB5 mov     eax, edi
00402AB7 lea     edi, [ebp+var_154]
00402ABD mov     byte ptr [ebp+var_4], 0Dh
00402AC1 call    sub_4044E1
00402AC6 push    offset aEncrypted ; "&encrypted="
00402ACB push    eax
00402ACC lea     eax, [ebp+var_1FC]
00402AD2 mov     byte ptr [ebp+var_4], 0Eh
00402AD6 call    sub_4044AA
00402ADB add     esp, 40h
00402ADE mov     ecx, eax
00402AE0 mov     eax, [ebp+arg_4]
00402AE3 lea     edi, [ebp+var_11C]
00402AE9 mov     byte ptr [ebp+var_4], 0Fh
00402AED call    sub_4044E1
00402AF2 push    offset aFailed  ; "&failed="
00402AF7 push    eax
00402AF8 lea     eax, [ebp+var_AC]
00402AFE mov     byte ptr [ebp+var_4], 10h
00402B02 call    sub_4044AA
00402B07 mov     ecx, eax
00402B09 mov     eax, [ebp+var_14]
00402B0C lea     edi, [ebp+var_E4]
00402B12 mov     byte ptr [ebp+var_4], 11h
00402B16 call    sub_4044E1
00402B1B push    offset aLength  ; "&length="
00402B20 mov     byte ptr [ebp+var_4], 12h
00402B24 push    eax
```

Figure N

certaines versions de Locky ajoutent les métadonnées d'un fichier à la fin du fichier lui-même avant de le chiffrer, ces informations seront essentielles pour l'opération de déchiffrement une fois la rançon payée. voici le structure ajoutée à la fin du fichier:

```
struct file_data
{
uint32_t start_marker;          //Structure start marker = 0x8956FE93
char id[16];                    //Infection ID
uint8_t aes_key[256];           //AES key encrypted with RSA-2048
uint32_t name_marker;           //Name start marker encrypted with AES (= 0xD41BA12A after decryption)
uint8_t orig_name[520];         //Original file name encrypted with AES
WIN32_FILE_ATTRIBUTE_DATA attr; //Original file attributes encrypted with AES
};
```

5.3.6 La Demande de Rançon

Comme pour tous les autres ransomwares, la victime peut s'attendre à voir une note de rançon l'informant des emplacements où elle peut accéder aux sites de paiement, afin de payer la rançon en échange d'un software pour déchiffrer ses fichiers. Locky présente cette note de rançon comme une image bitmap affichée à la victime comme un wallpaper (Figure O) ainsi qu'un fichier texte dans le Bloc-notes sous le nom de "_Locky_recover_instructions.txt".

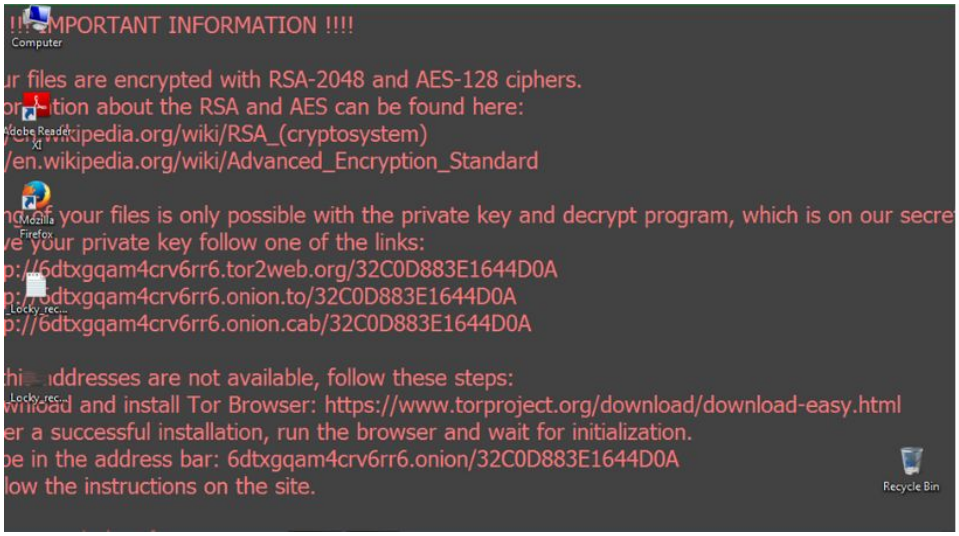


Figure O

L'infrastructure de paiement repose sur les fournisseurs proxy Tor2Web populaires tels que Tor2Web.org et onion.cab pour fournir aux victimes l'accès à leurs sites de paiement hébergés par Tor.
Tous ces URLs redirigeront la victime vers l'adresse oignon "6dtxgqam4crv6rr6.onion", où elle trouve une multitude de façons et d'instructions pour l'aider à acheter des Bitcoin, ainsi que l'adresse à laquelle elle doit envoyer la rançon(0.5 Bitcoin).
L'adresse Bitcoin à laquelle il faut envoyer la rançon change d'un PC infecté à un autre, probablement pour aider à masquer les transactions et à rendre plus dure la tâche aux investigateurs.

Contrairement aux anciens ransomwares, l'image de fond d'écran et le fichier texte qui annoncent la mauvaise nouvelle aux utilisateurs des PCs infectés ne sont pas contenus dans le binare du malware(comme on l'a vu avec Lorobot) mais ces fichiers sont transférés depuis les serveurs C&C.

Locky commence par détecter la langue utilisée par le système avec la fonction windows GetUserDefaultUILanguage, ensuite il transfère cette information au serveur, ce dernier dispose du même message(qui annonce l'infection) dans différentes langues, et renvoie à Locky le binaire du message dans la langue du système.

Comme le montre la portion de code de la Figure P, une fois le binaire du message reçu, Locky commence à créer le wallpaper avec les fonctions systèmes CreateSolidBrush, FillRec,SetTextColor...

Figure P(avec ollydbg)

Une fois l'image créée, Locky la met comme image de fond d'écran, avec SystemParamsInfo et avec l'argument 0x14(= SPI_SETDESKWALLPAPER) comme le montre le code dans la figure Q, exactement de la même manière que Lorobot.

```
004039BD push    3
004039BF push    eax             ; pvParam
004039C0 push    ebx             ; uiParam
004039C1 push    14h             ; uiAction
004039C3 call    ds:SystemParametersInfoW
004039C9 cmp     [ebp+var_58], 8
```

Figure Q

Déchiffrement avec Ranson

À l'intérieur des notes de rançon de Locky se trouvent des liens vers un site Tor appelé la page Locky Decrypter. Cette page se trouve à 6dtxgqam4crv6rr6.onion et contient la quantité de bitcoins à envoyer comme paiement, la façon d'acheter les bitcoins et l'adresse bitcoin à laquelle la victime doit effectuer le paiement. Une fois qu'une victime envoie le paiement à l'adresse bitcoin attribuée, cette page fournira un software déchiffreur qui peut être utilisé pour décrypter ses fichiers. Ce software se basera sur les fichiers Logs et la clé privée du serveur.

5.3.7 Résumé

Ce schéma(R) retrace les grandes lignes du fonctionnement du ransomware Locky.

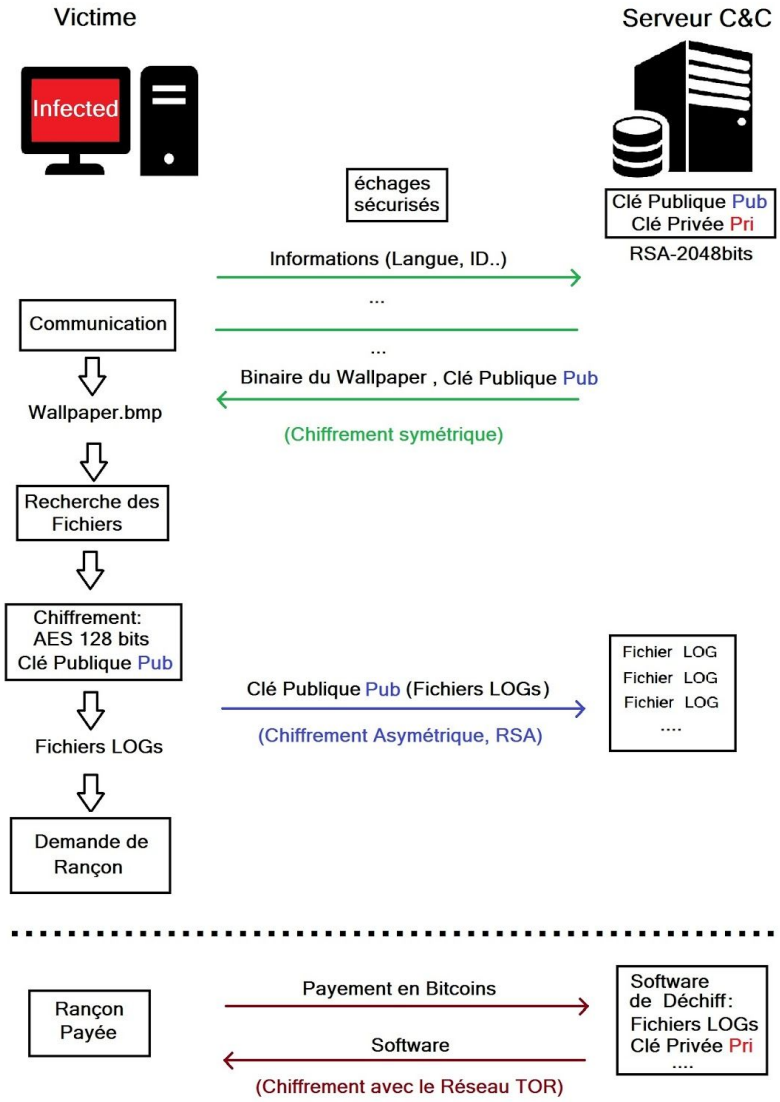


Figure R

Liens Locky:
https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/26000/PD26383/en_US/McAfee_Labs_Threat_Advisory_Ransomware-Locky.pdf

https://blog.malwarebytes.com/threat-analysis/2016/03/look-into-locky/
https://blog.malwarebytes.com/security-world/2012/09/so-you-want-to-be-a-malware-analyst/
https://blog.cylance.com/cracking-ransomware
https://www.proofpoint.com/us/threat-insight/post/Locky-Ransomware-Cybercriminals-Introduce-New-RockLoader-Malware
https://securelist.com/blog/research/74398/locky-the-encryptor-taking-the-world-by-storm/

Binaire de Locky:
https://www.hybrid-analysis.com/sample/49a48d4ff1b7973e55d5838f20107620ed808851231256bb94c85f6c80b8ebfc?environmentId=100

Misc magazine: No 55, 28, 43

CHAPITRE III
La Lutte Contre Les Ransomwares

1. La prévention

Objectif: Considérant que la prévention réduit considérablement les risques d'attaques et de menaces, je passerai en revue, dans cette partie, un ensemble de précautions à prendre, des recommandations à suivre et ce, pour assurer une prévention basique, avancée et celle à adopter par les entreprises.

1.1 Prévention (Basique)

Pour réduire considérablement les risques d'être piégé, il serait très utile de suivre les recommandations suivantes ;

1) Ne jamais cliquer sur les pop-up (installer une extension qui les bloque sur votre navigateur, Adblock par exemple).
2) Assurez-vous que votre système d'exploitation, vos navigateurs, Firewall(s), Antivirus, et vos Logiciels sont à jour et /corrigés. Activez la mise à jour automatique de ces systèmes et softwares.
3) Ne jamais répondre aux courriers indésirables (Spam).
4) N'ouvrez que les pièces jointes connues ou prévues.
5) Ne cliquez pas sur les liens dans les courriels. Toujours copier et coller les liens dans la barre d'URL du navigateur.
6) Évitez d'utiliser votre compte de messagerie personnel/professionnel pour vous inscrire à des services peu connus, pas fiables ou à court terme.
7) Évitez de télécharger des fichiers avec des programmes de téléchargement sur réseau peer-to-peer (P2P).
8) Utilisez un conseiller de site fiable, tel que McAfee SiteAdvisor, pour vous aider à éviter les sites potentiellement malveillants.
9) Ne pas utiliser le même poste de travail pour l'usage personnel et pour le travail.

10) Sauvegardez régulièrement vos données (Backup). Ne pas les sauvegarder sur des serveurs de stockage réseau comme les NAS, et ne pas se contenter des VSS (Shadow Copy Service) de windows, car certains Ransomwares peuvent chiffrer les données des PCs/Serveurs qui se trouvent dans le même intranet que le PC a infecer.
11) Utilisez un disque dur externe pour vos sauvegardes. Débranchez le lecteur après avoir fini de copier les fichiers (et testez le).
12) Utilisez des antivirus de type Anti-Ransomware (en même temps que votre antivirus de base), comme : WinPatrol, HitmanPro.Alert, Malwarebytes anti ransomware...

1.2 Prévention Avancée

A côté des recommandations précédentes, il serait judicieux, voire nécessaire, de suivre les consignes suivantes ;

1) Conservez toujours UAC (*User Account Control*) activé. Un certain nombre d'opérations effectuées par crypto-ransomware nécessitent les droits Admin, un processus a le même niveau d'accès aux données que celui dont dispose l'utilisateur, par conséquent, des informations sensibles peuvent facilement être supprimées ou transmises hors de l'organisation si un utilisateur exécute intentionnellement ou involontairement des logiciels malveillants, l'UAC permet de définir pour chaque programme qui est lancé un niveau de privilèges indépendant des droits possédés par l'utilisateur actif. Lorsque UAC est activé, tous les utilisateurs (même ceux qui possèdent des privilèges d'administration) possèdent par défaut des droits identiques à ceux des utilisateurs limités.

2) Travaillez à partir du principe de la moindre permission.

3) Évitez le partage des données en réseau local, mais si vous êtes obligés de le faire, créez des dossiers cachés pour le partage réseau (*Hidden Network Share*), pour cela il suffit d'ajouter le symbole "$" à la fin du nom du dossier à partager (sans espace) afin de les rendre "invisibles" à la fonction *WNetOpenEnum()*, car beaucoup de Ransomwares utilisent la fonction *WNetOpenEnum()* de l'API Widows pour lister les ressources partagées pour les chiffrer aussi.

Par Exemple, ici le Dossier partagé est nommé "C$"

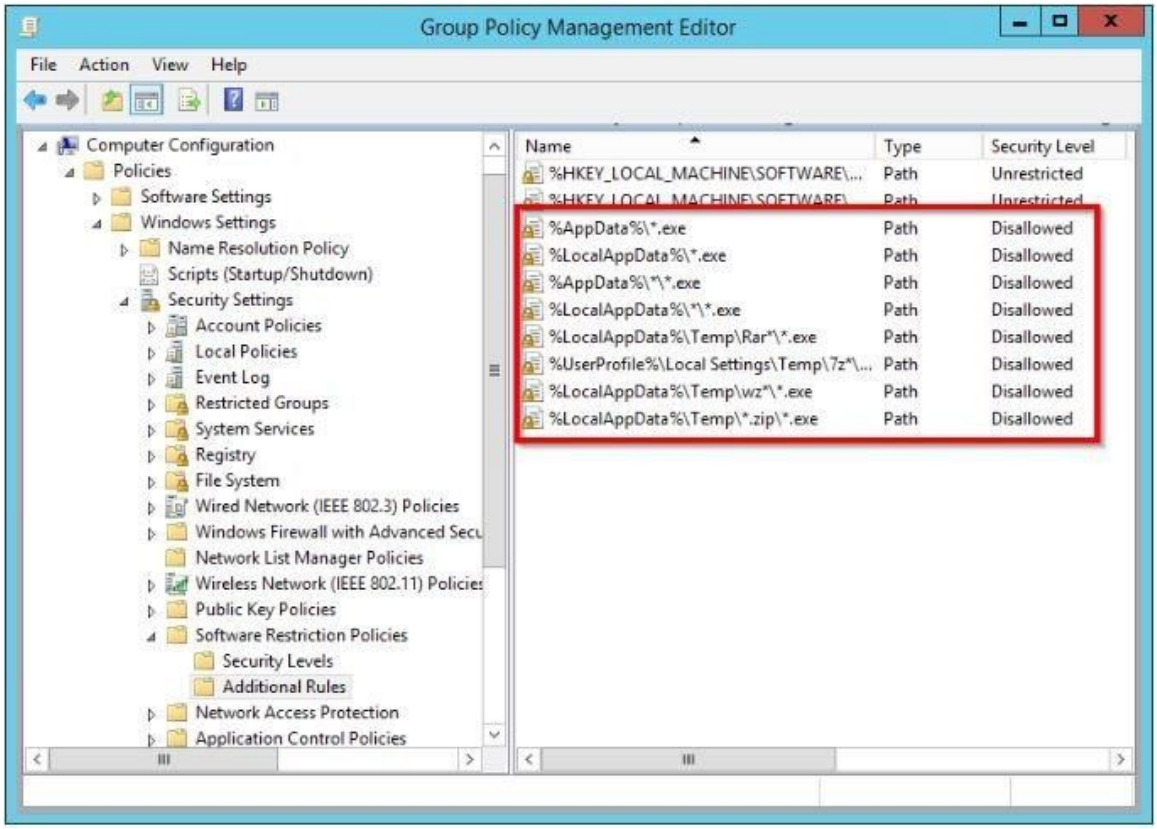
Pour plus d'informations sur le Hidden Network Share : *http://www.online-tech-tips.com/computer-tips/how-to-create-a-windows-xp-hidden-folder-share/*

4) Utilisez l'outil SRP (Software Restriction Policies) de Windows, ou un outil comme Applocker (similaire à SRP et permet de gérer un parc de PCs, idéal pour les organisations mais pas compatible avec toutes les versions de Windows).
SRP permet de créer des règles qui permettent de restreindre les types de fichiers ou des exécutables qui peuvent être manipulés/exécutés sur un PC,

Le Modèle BlackList: Le modèle de liste Noire exige que l'Admin système soit constamment réactif aux nouvelles menaces en mettant à jour les règles SRP.

Un exemple de règle:
Paths: %AppData%*.exe
Security Level: Disallowed
Description: "Don't allow executables to run from immediate subfolders of %AppData%."

Cette règle bloque l'exécution des ".exe" qui se trouvent dans la variable d'environnement "*%AppData%*", on répète la même chose pour %LocalAppData%*.exe, %LocalAppData%TempRar**.exe, %LocalAppData%Temp7z**.exe...

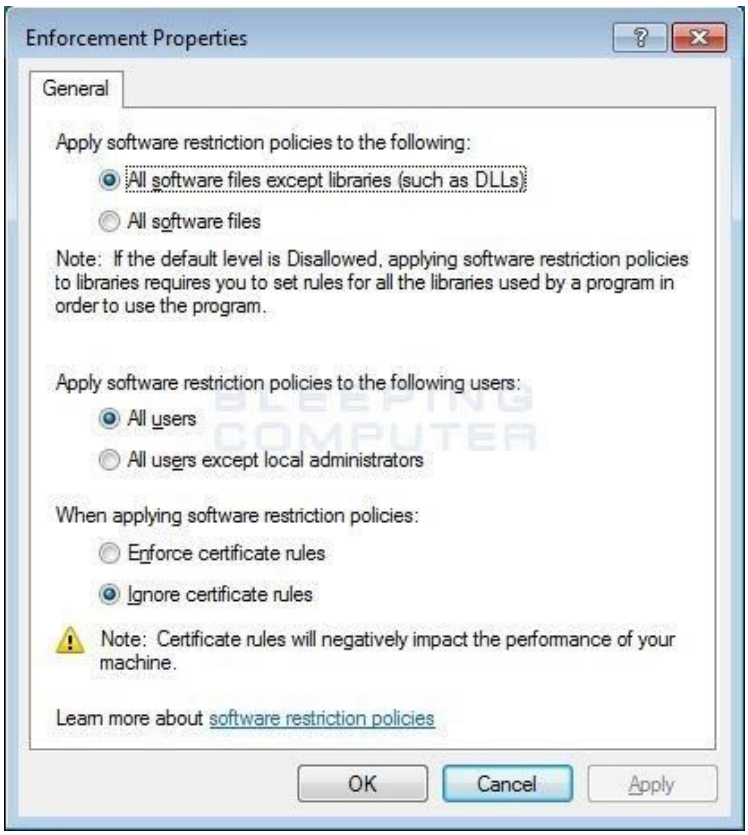


Exemple d'un ensemble de Règles

Pour plus d'informations sur l'outil SRP(et la Blacklist) : https://blog.brankovucinec.com/2014/10/24/use-software-restriction-policies-to-block-viruses-and-malware/

Le Modèle Whitelist :

Ouvrez le *Local Security Policy,* clic droit sur *software restriction policy ->New Software Restriction Policies -> Enforcement -> ...*



Pour plus d'informations sur la création d'une Whitlist:
https://www.bleepingcomputer.com/tutorials/create-an-application-whitelist-policy-in-windows/

La plupart des ransomwares exécutent des binaires malicieux depuis % AppData% et %LocalAppData% , mais de nouveaux Ransomwares utilisent d'autres emplacements pour s'exécuter, avec le modèle *Blacklist* il faut ajouter de nouvelles règles chaque fois que de nouveaux Malwares (utilisant d'autres dossier) apparaissent, par contre avec le modèle *Whitelist*, ils suffit d'ajouter de nouvelles règles chaque fois que vous installez un nouveau programme (une règle autorisant notre nouveau programme à s'exécuter), c'est pour cela que le modèle basé sur une *WhiteList* est recommandé.

5) Évitez Le *Mapping* des disques durs.

Le Mapping: Consiste à connecter une partition du disque dur physique de votre PC à des données/dossiers partagés stockés dans un autre PC/Serveur.
Pour plus d'informations sur le Mapping :
http://www.it.cornell.edu/services/guides/computer/howto/map_win7.cfm

On dit que la meilleure défense c'est l'attaque, mais en *Sécurité des Systèmes d'Information* la légitime défense n'est pas autorisée, au jour d'hui l'état de la technique et le cadre juridique ne le permettent pas (identifier les attaquants, quelles cibles sont autorisées, puissance de la riposte..), il faut donc faire avec ces contraintes et se contenter pour le moment de bien se défendre.

1.3 Prévention pour les entreprises

Elle est cruciale et doit être, de ce fait, rigoureusement assurée, pour ce faire, l'observation des recommandations suivantes est nécessaire ;

1) Le Back-up est obligatoire, le chiffrement peut atteindre des fichiers importants pour le travail de l'entreprise, s'il est techniquement impossible de sauvegarder tous les fichiers, choisissez les plus critiques (documents comptables, documents juridiques, les données des clients), isolez-les et sauvegardez-les régulièrement en utilisant des méthodes de Sauvegardes Incrémentales par exemples.
2) Utilisez des solutions de sécurité fiables, utilisez les configurations avancées que proposent ces produits (ne pas se contenter des configurations par défaut).
3) Sensibilisez votre personnel: souvent l'infection par Ransomware résulte d'un manque de connaissance du personnel sur ces types de menaces et leur fonctionnement.
4) Gérez de façon centralisée les mises à jours des PCs de la boîte, en utilisant un logiciel comme *WSUS* pour Windows.
5) Optez pour une application robuste et sécurisée de type BYOD si vos personnels utilisent leurs propres PCs ou SmartPhones pour accéder aux ressources de l'entreprise, pour que ces appareils ne seront pas être utilisés comme des points d'entrées pour l'infection des données de l'entreprise.
6) Evitez de payer les rançons, et signaliez l'attaque à la police.
7) Appliquez les mesures décrites dans les points précédents (*Prévention Basique et Avancée*)

2. La lutte contre les ransomwares, les perspectives

Dans les années à venir, les ransomwares continueront encore d'attaquer et le butin récolté par ce malware sera plus consistant.
D'une part, les développeurs de ces ransomwares vont, pour bien mener leurs attaques, adapter ces derniers et les améliorer pour contourner les mesures de sécurité, et pour ce faire, ils utiliserons de nouvelles techniques et exploiteront les éventuelles nouvelles failles qui risquent de se trouver au niveau de toutes les étapes (diffusion, chiffrement, etc..).

Une des solutions serait que dans un futur proche, les constructeurs d'ordinateurs opteront pour l'utilisation de la notion de Cloud, même avec tous leurs clients, en commercialisant des pc sans disques durs (juste la mémoire nécessaire pour le fonctionnement de l'OS.)
Ainsi, l'utilisateur aura un accès distant (via Internet) à son espace de stockage et des spécialistes géreront, à sa place, la sécurité de ses données.
Les spécialistes recommandent tous d'avoir recours aux backups, assurant, de la sorte, une duplication des données dans un espace non connecté à la machine de cet utilisateur (ou à son réseau) tels que des disques durs externes.

Les laboratoirs de Kaspersky ont lancés l'initiative No More Ransom qui est née du désir d'aider les victimes de ransomware à récupérer leurs données chiffrées sans avoir à payer de criminels, ils mettent à disposition des victimes des softwares pour déchiffrer les données, la liste des softwares est constamment mise à jour: https://noransom.kaspersky.com/

Conclusion:

L’évolution, loi immuable inscrite dans la nature des choses, est le ressort qui pousse l’Homme à rechercher le meilleur.
Dans ce cadre, le projet de semestre est une occasion offerte aux futurs ingénieurs pour montrer le degré de maturité atteint et le niveau d’une prise de conscience de la nécessité de soumettre les dispositifs et les méthodes à une analyse critique.
Tout au long de l’expérience passionnante que constitue l’élaboration de mon projet, je me suis surpris, plus d’une fois, en train d’imaginer une nouvelle solution ou de rêver une énième amélioration. Réapprendre à imaginer, à rêver et à être évolutif est, pour moi, le meilleur profit que j’ai pu tirer de mes études et de ma formation…

Tout au long de l’élaboration du présent rapport, je me suis trouvé, plus d’une fois, devant un choix contraignant, surtout quand il s’est agi de s’attaquer à la partie technique, qui constitue le cœur de mon projet : «Mise en œuvre, analyse et monitoring d’un ransomware ».
Lequel des ransomwares choisir ? GpCode, Lorobot, CTB-Locker, CryptoLocker, Teslacrypt, Petya, Locky.. ?
J’ai commencé par étudier Lorobot, un ancien ransomware assez simple afin de me familiariser avec les outils du reverse engineering et le langage assembleur X86.
Les ransomwares des ces dernières années se ressemblent entre eux, mais j’ai analysé plus en détail Locky vu qu’il est le dernier en date au moment de l'élaboration du rapport. Alors Lorobot ou Locky ? Le premier étant plus ancien que le second mais utilisant des techniques intéressantes. Le deuxième utilisent les techniques les plus élaborées. Finalement les deux figureront dans ce mémoire.

Si la première partie du rapport a servi d’introduction, la seconde peut être considérée comme l’axe central de ce projet. Dans la dernière partie, l’essentiel de la lutte efficace contre les rançongiciels s’est focalisé sur la prévention, qu’elle soit basique, avancée ou destinée pour les entreprises.

Chaque jour, de nouveaux ransomwares sont créés, ce qui implique que la lutte contre eux doit être une action continue. Éradiquer la menace des ransomwares est un long chemin à parcourir. Ce n'est qu'en recueillant des preuves solides et des statistiques concrètes sur le problème que nous pourrons évaluer nos options de manière appropriée. Malheureusement, ce ne sont pas toutes les personnes concernées par le ransomware qui signalent l'incident, et même celles qui le font, en rendent compte à différentes institutions, ce qui rend difficile la collecte d'un ensemble complet de données.