Analyse de Malware

LOCKY

Réalisé par: Guillaume COUCHARD, Adrien COUERON, Gabriel DIOUF, Kévin FAUVE

Encadré par: Guillaume CHOUQUET, Vianney LAPOTRE

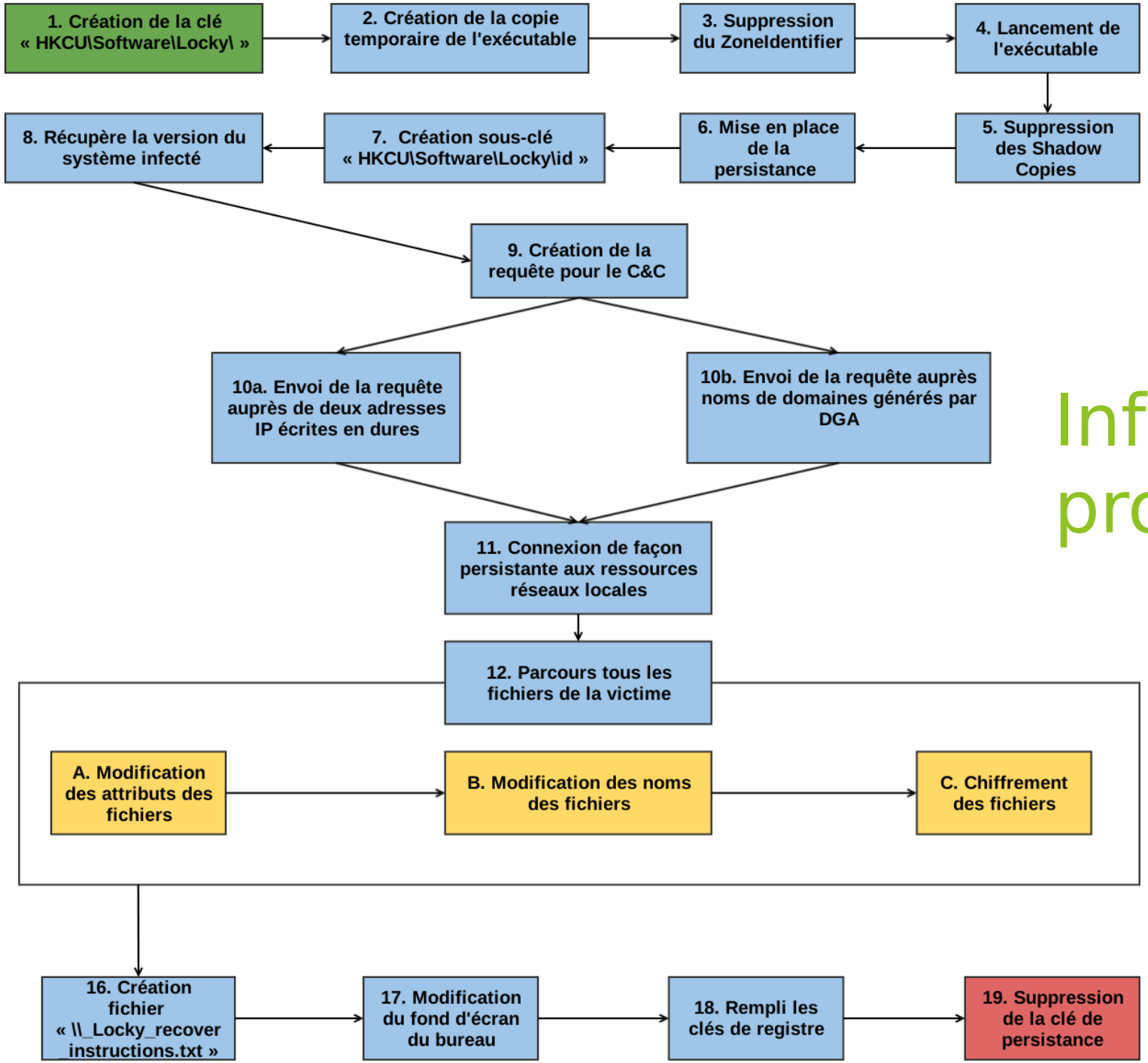
ENSIBS VANNES – Cyberdéfense – 2ème Année

Table of contents

Malware presentation

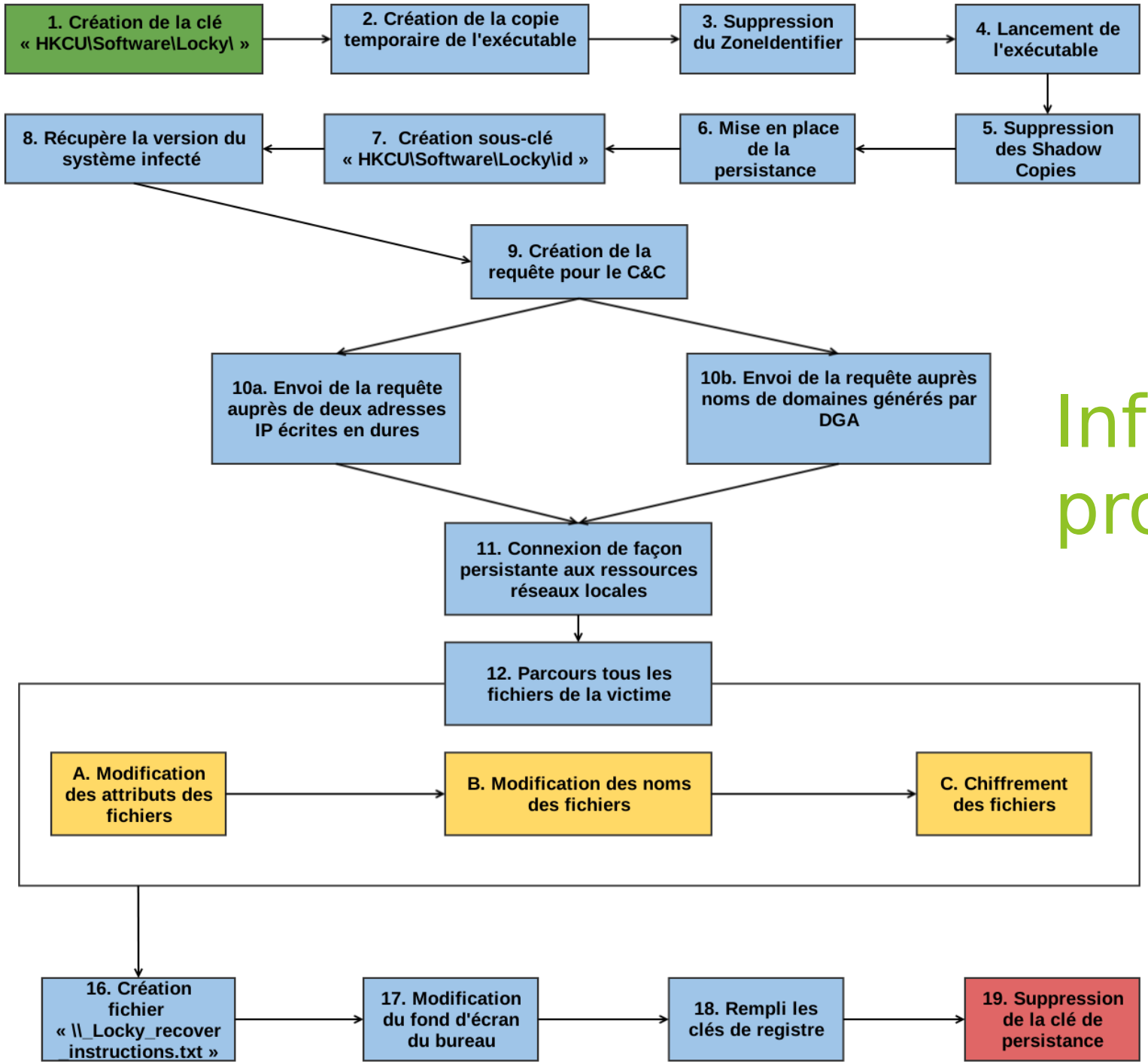
- Crypto ransomware
- February 2016
- Russian
  - If(lang == “RU”){ exit(0); }
- Distributed by spam
  - Macro word
  - Javascript file in zip archive

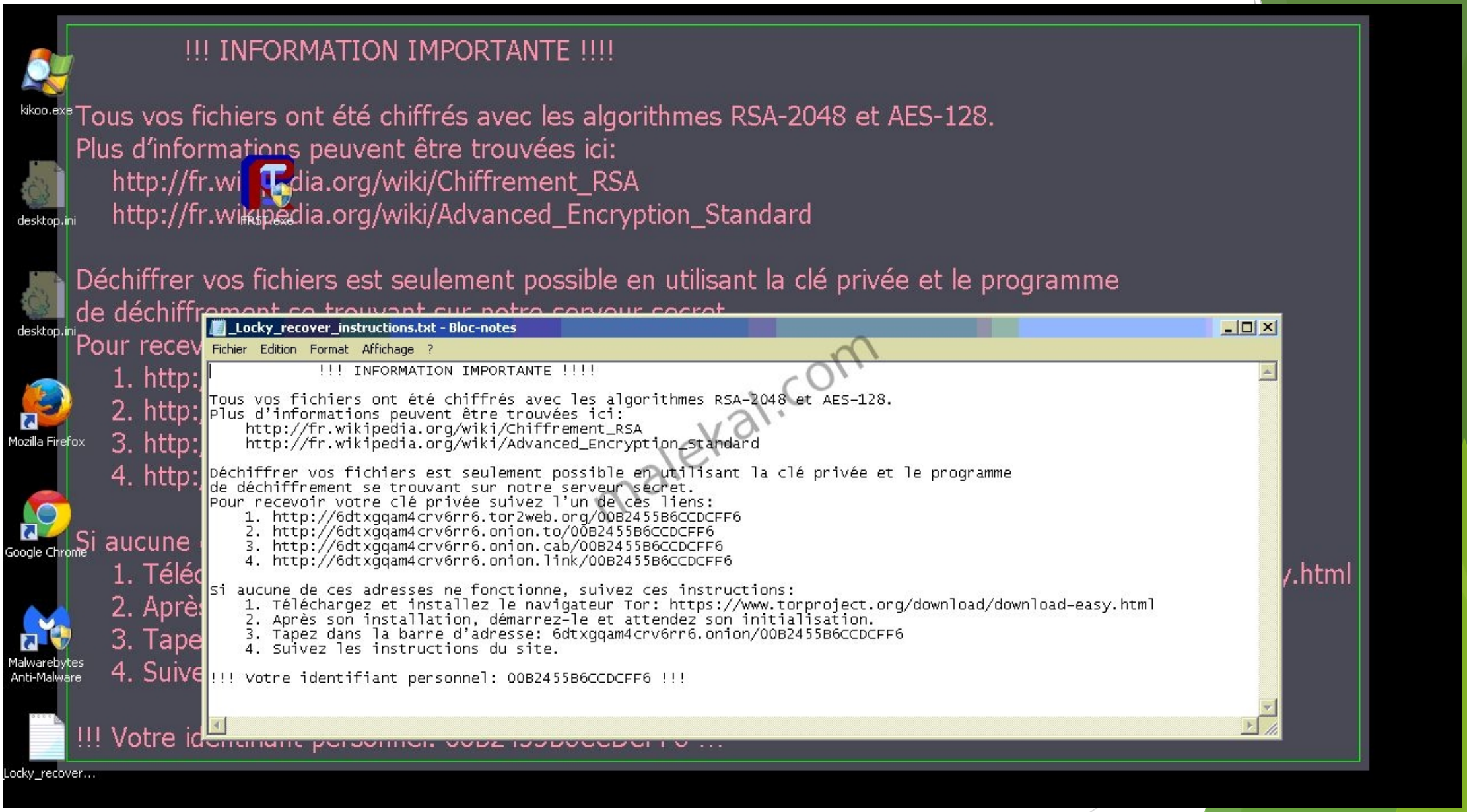
Infection procedure



.m4u	.avi	.qcow2	.bak	.bmp	.psd	.brd	.cpp	.db	.sldm	.uop	.sxi	.xlsm	.ots	.max	.stw
.m3u	.asf	.vdi	.tar	.png	.cmd	.sch	.php	.mdb	.sldx	.potx	.otp	.xlsb	.ods	.3ds	.sxw
.mid	.mpeg	.vmdk	.tgz	.gif	.bat	.dch	.ldf	.sql	.ppsm	.potm	.odp	.slk	.hwp	.xml	.ott
.wma	.vob	.vmx	.gz	.raw	.sh	.dip	.mdf	.SQLITEDB	.ppsx	.pptx	.wb2	.xlw	.602	.txt	.odt
.flv	.mpg	.gpg	.7z	.cgm	.class	.pl	.ibd	.SQLITE3	.ppam	.pptm	.123	.xlt	.dotm	.CSV	.DOC
.3g2	.wmv	.aes	.rar	.jpeg	.jar	.vbs	.MYI	.asc	.docb	.std	.wks	.xlm	.dotx	.uot	.pem
.mkv	.fla	.ARC	.zip	.jpg	.java	.vb	.MYD	.lay6	.mml	.sxd	.wk1	.xlc	.docm	.RTF	.p12
.3gp	.swf	.PAQ	.djv	.tif	.rb	.js	.frm	.lay	.sxm	.pot	.xltx	.dif	.docx	.pdf	.csr
.mp4	.wav	.tar.bz2	.djvu	.tiff	.asp	.asm	.odb	.ms11 (SC)	.otg	.pps	.xltm	.stc	.DOT	.XLS	.crt
.mov	.mp3	.tbk	.svg	.NEF	.cs	.pas	.dbf	.ms11	.odg	.sti	.xlsx	.sxc	.3dm	.PPT	.key

Infection procedure




!!! INFORMATION IMPORTANTE !!!!
Tous vos fichiers ont été chiffrés avec les algorithmes RSA-2048 et AES-128.
Plus d'informations peuvent être trouvées ici:
http://fr.wikipedia.org/wiki/Chiffrement_RSA
http://fr.wikipedia.org/wiki/Advanced_Encryption_Standard
Déchiffrer vos fichiers est seulement possible en utilisant la clé privée et le programme
de déchiffrement se trouvant sur notre serveur secret.
Pour recev
1. http:
2. http:
3. http:
4. http:
Si aucune
1. Téléc
2. Aprè
3. Tape
4. Suive
.html
!!! Votre id
kikoo.exe
desktop.ini
FRST.exe
desktop.ini
Mozilla Firefox
Google Chrome
Malwarebytes Anti-Malware
Locky_recover...
_Locky_recover_instructions.txt - Bloc-notes
Fichier Edition Format Affichage ?
!!! INFORMATION IMPORTANTE !!!!
Tous vos fichiers ont été chiffrés avec les algorithmes RSA-2048 et AES-128.
Plus d'informations peuvent être trouvées ici:
http://fr.wikipedia.org/wiki/Chiffrement_RSA
http://fr.wikipedia.org/wiki/Advanced_Encryption_Standard
Déchiffrer vos fichiers est seulement possible en utilisant la clé privée et le programme
de déchiffrement se trouvant sur notre serveur secret.
Pour recevoir votre clé privée suivez l'un de ces liens:
1. http://6dtxgqam4crv6rr6.tor2web.org/00B2455B6CCDCFF6
2. http://6dtxgqam4crv6rr6.onion.to/00B2455B6CCDCFF6
3. http://6dtxgqam4crv6rr6.onion.cab/00B2455B6CCDCFF6
4. http://6dtxgqam4crv6rr6.onion.link/00B2455B6CCDCFF6
Si aucune de ces adresses ne fonctionne, suivez ces instructions:
1. Téléchargez et installez le navigateur Tor: https://www.torproject.org/download/download-easy.html
2. Après son installation, démarrez-le et attendez son initialisation.
3. Tapez dans la barre d'adresse: 6dtxgqam4crv6rr6.onion/00B2455B6CCDCFF6
4. Suivez les instructions du site.
!!! Votre identifiant personnel: 00B2455B6CCDCFF6 !!!

Locky Decryptor™

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

Comment acheter Locky Decryptor™?

1 Vous avez la possibilité de payer en bitcoints, on peut les obtenir par des voies différentes.

2 Il vous faut enregistrer un portefeuille:

Le plus simple portefeuille ou autres moyens de création de portefeuille.

3 Malgré le fait qu'il n'est pas si simple d'obtenir des bitcoints, leur achat devient moins compliqué de jour en jour.

Nos recommandations:

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

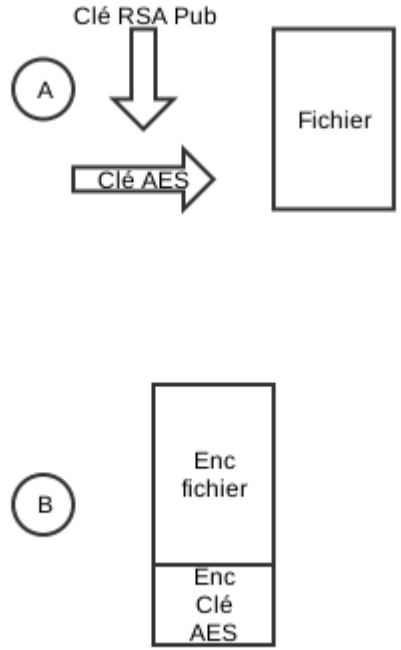
4 Envoyez 0.5 BTC sur la bitcoint adresse:

1JmS3Z4s45pHFjYchftqKmNXWfqgDdQXaH

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

File encryption

- Getting RSA public key from C&C
- For each file, generation AES key
- File encryption with AES key
- AES key encryption with RSA key
- Concatenate file with AES key



Domain Generation Algorithm

- Enable to generate dynamically C&C domains names

- In case of Locky
  - 6 different domains names at same time
  - Renew every 2 days
  - From 5 to 16 chars [a-y]
  - Followed by TLD among 14 preset

Reverse du DGA

```
#Configuration du sample
class Config:
        rotate = 5
        modulo = 6
        const1 = 0xB11924E1
        const2 = 0x1BF5
        const3 = 0x27100001
        const4 = 0x2709A354
        lang = ['ru', 'pw', 'eu', 'in', 'yt', 'pm', 'us', 'fr', 'de', 'it', 'be', 'uk', 'nl', 'tf']

#Generation des 6 domaines pour la date donnee
for numDomaine in range(6):
        #Recuperation de la date pour chaque round
        day = d.day
        year = d.year
        month = d.month

        #Traitement sur les donnees de date et de configuration
        data = ror(Config.const1 * (year + Config.const2), Config.rotate)
        data = ror(Config.const1*(day // 2 + data + Config.const3), Config.rotate)
        data = ror(Config.const1*(month + data + Config.const4), Config.rotate)
        numDomaineMod = rol(numDomaine % Config.modulo, 21)
        data = ror(Config.const1*(numDomaineMod + data + Config.const3), Config.rotate) + Config.const3

        #Choix de la longueur du nom de domaine
        length = (data % 11) + 5
        #Generation de chaque caractere
        domain = ""
        for i in range(length):
                data = (ror(Config.const1 * rol(data, i), Config.rotate) + Config.const3) & 0xFFFFFFFF
                domain += chr((data % 25) + ord('a'))

        #Ajout du TLD
        domain += '.'
        numTld = ror(data * Config.const1, Config.rotate) + Config.const3
        domain += Config.lang[(numTld) % len(Config.lang)]

        print domain
```

Nice cert !

From Thomas Fleitour <Thomas.Fleitour@univ-ubs.fr>

Subject **Infection Malware Locky !** 16/03/2016 15:15

To Me <coueron.e1504488@etud.univ-ubs.fr>

Bonjour,

Je suis Thomas Fleitour du service informatique de l'UBS, responsable
adjoint de la Sécurité du Système d'Information.

Le Cert Renater nous informe ce jour que votre machine est suspectée
d'être infectée par le Malware Locky.

En attendant que vous procédiez à la désinfection, je bannis temporairement votre
machine du réseau eduroam de l'UBS.

Merci de prendre quelques minutes pour me contacter par téléphone.

Cordialement,

Objet: Contact téléphonique !
De: "Thomas Fleitour" <Thomas.Fleitour@univ-ubs.fr>
Date: Mar 24 mai 2016 16:06
À: couchard.e1405447@etud.univ-ubs.fr
Create Filter: Automatically | From | To | Subject
Options: Afficher l'en-tête complet | Voir la version imprimante | Téléc

Bonjour,

Je suis Thomas Fleitour du service informatique de l'UBS, responsable
adjoint de la Sécurité du Système d'Information.

Le Cert Renater nous informe ce jour que votre machine est suspectée
d'être infectée par le ransomware locky.

En attendant votre appel, je bannis temporairement votre
machine du réseau eduroam de l'UBS.

Merci de prendre quelques minutes pour me contacter par téléphone.

Cordialement,