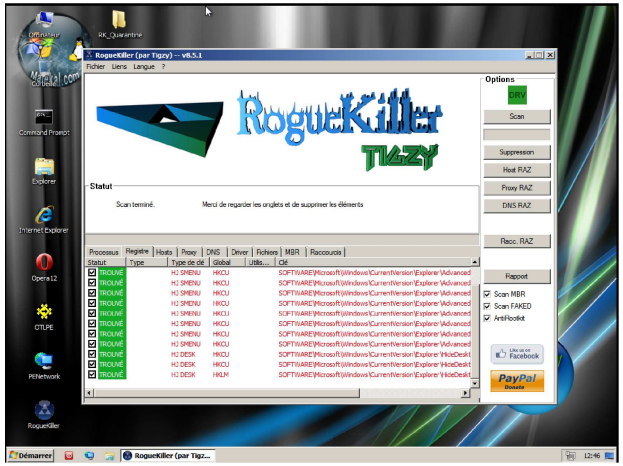
- *NE PAYEZ PAS c'est une escroquerie !*

*Pour supprimer ce **Virus** ou **Trojan** qui infecte votre machine, suivant votre système d'exploitation (**XP, vista ou Seven, ...**)*

*1 = Essayez de démarrer en **mode sans échec avec prise en charge réseau** (tapoter la touche F8 durant le démarrage de votre PC), si cela fonctionne vous pouvez accéder à votre bureau et télécharger un utilitaire pour soigner l'infection.*

Rendez vous sur le site
www.malekal.com



Suivez les indications en fonction de l'infection subie.

***D**epuis le mois de décembre 2011,*

des centaines d'internautes en France, mais aussi dans de nombreux pays européens ou extérieurs à l'Europe
– notamment les Etats-Unis –
sont victimes de virus informatiques nommés « rançongiciels ».
Ces virus bloquent totalement le fonctionnement de l'ordinateur, affichent une page d'information se réclamant d'un service de police local et exigent le paiement d'une amende pour obtenir le déblocage du système. Dans certains cas, les fichiers personnels de l'utilisateur peuvent faire l'objet d'un chiffrement les rendant inutilisables.
Le phénomène semble se développer dans des proportions importantes.

***D**ébut 2013,*

la division de lutte contre la cybercriminalité a ainsi été informée de 980 plaintes et 127 procès-verbaux de renseignement judiciaire (ZGN/ZPN).

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

Gendarmerie nationale
MINISTÈRE DE L'INTÉRIEUR

Lutte contre les escroqueries sur INTERNET

ENQUETEUR TECHNOLOGIES NUMERIQUES
N-TECH
GENDARMERIE NATIONALE

Cybercriminalité

NE PAYEZ PAS !

Gendarmerie nationale
MINISTÈRE DE L'INTÉRIEUR

Mode opératoire :

- 1 =Contamination de l'ordinateur des victimes *les victimes sont redirigées par différents moyens (bandeaux publicitaires malveillants, liens dans des courriers électroniques non sollicités ou des messages sur des réseaux sociaux, ou encore scripts insérés dans des sites Web piratés) vers des sites Web appelés « Plateformes d'exploits » qui vont tester, selon la configuration de leur ordinateur, différentes vulnérabilités connues de leur navigateur Web ou des modules additionnels. Si une faille existe le virus est alors installé sur l'ordinateur.*

- 2 = Une image s'affiche en plein écran *et bloque l'usage de l'ordinateur avec un avertissement et un ordre de paiement pour débloquer la machine.*
(cf copie écran en page centrale de ce document)

3 = Collecte des informations de paiement :
en Europe, les modes de paiement couramment demandés sont des tickets Ukash ou Paysafecard que l'on peut acquérir dans les bureaux de tabac. Le code est imprimé sur un ticket remis à l'acheteur par le buraliste.

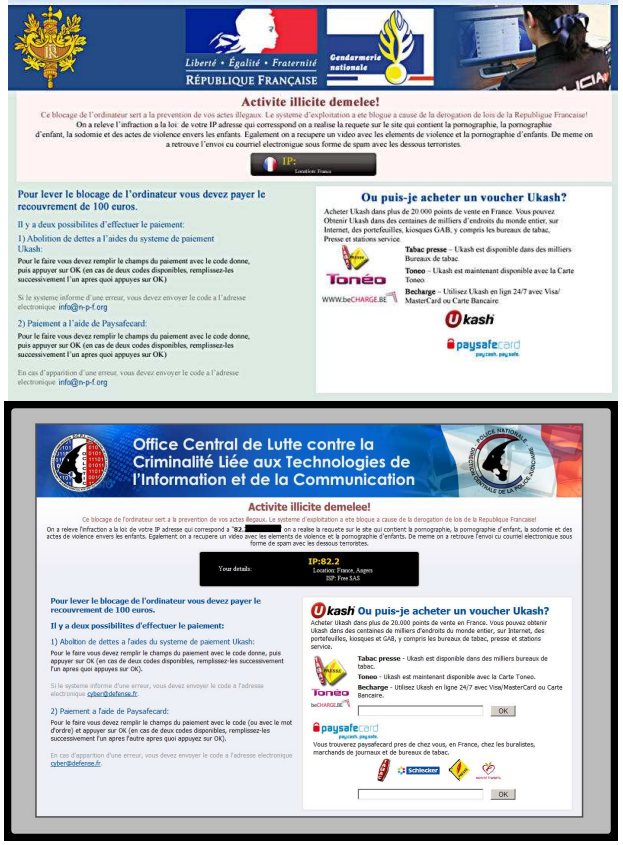
VIRUS POLICE GENDARMERIE
et autres rançongiciels :
La procédure de désinfection est disponible sur :

www.malekal.com.

Gendarmerie nationale
MINISTÈRE DE L'INTÉRIEUR

exemples de FAUSSES ALERTES
action de VRAIS VIRUS !

Figure 1 : copie d'écran d'un ordinateur bloqué par la variante « Goldenbaaks » des rançongiciels (03/2012).



© ***BDRIJ 26***