Flimrans : Ransomware Office Central de la lutte contre la criminalité lié aux technologies

Une nouvelle variante qui fait assez mal depuis plusieurs semaines.
J'ai eu du mal à avoir un dropper fonctionnel. Je remercie Kafeine pour l'aide.

La variante affiche une page de blocage Police de type Office Central de la lutte contre la criminalité lié aux technologies de l'information et de la communication, sans les logo HADOPI contrairement à d'autres variantes : https://www.malekal.com/2012/01/10/virus-hadopi-gendarmerie-office-central-lutte/

Son petit est nom est Flimrans – La fiche sur botnet.fr : https://www.botnets.fr/index.php/Flimrans

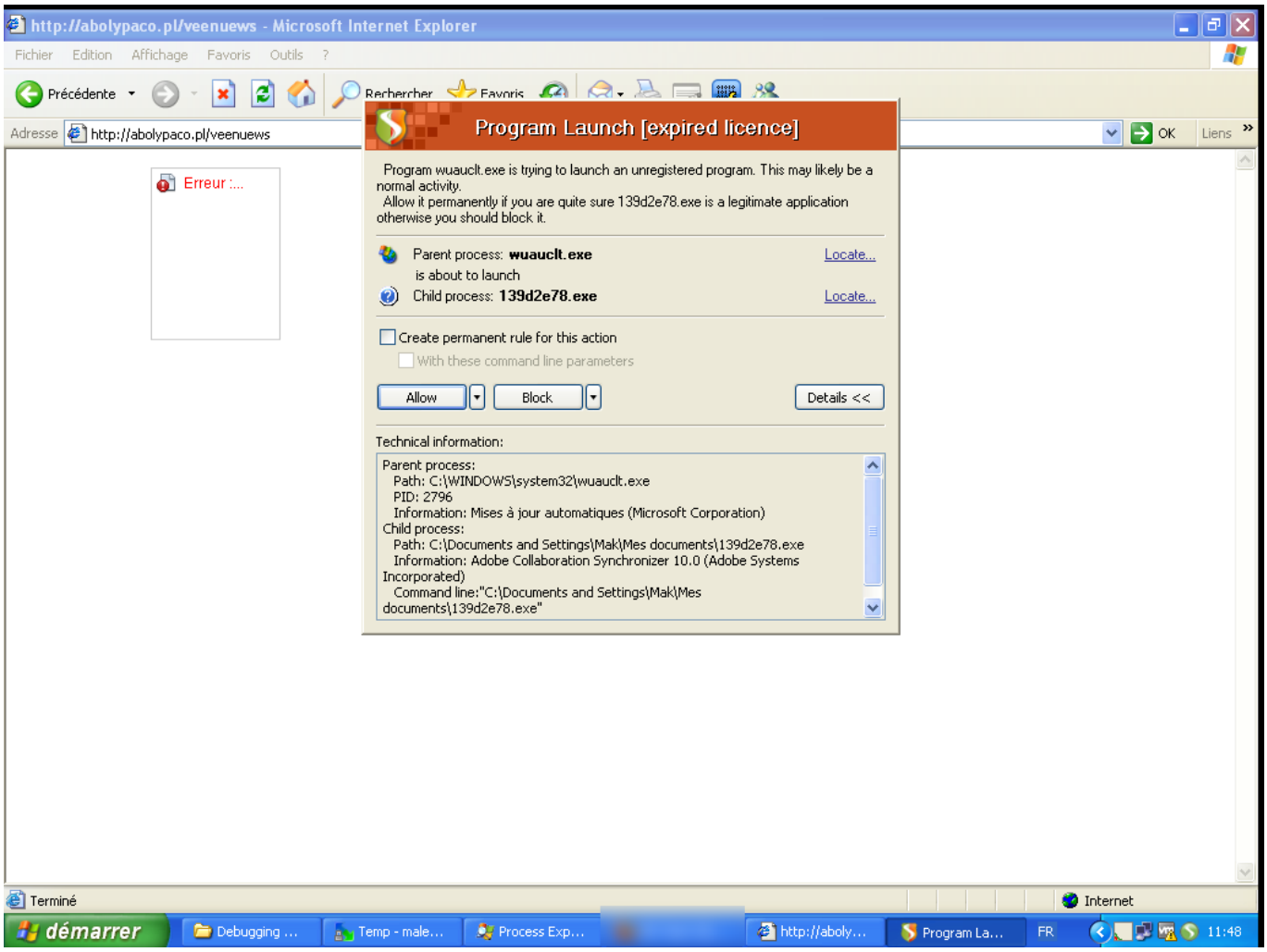
Exemple de campagne de malvertising qui charge le malware : https://www.malekal.com/2013/05/29/en-ero-advertising-malvertising-for-flimrans-ransomware-campaign/

Une capture d'écran de l'Exploit sur Site web qui lance le malware.
Le malware est un ransomware qui va télécharger ensuite le ransomware via le processus wuauclt.exe.

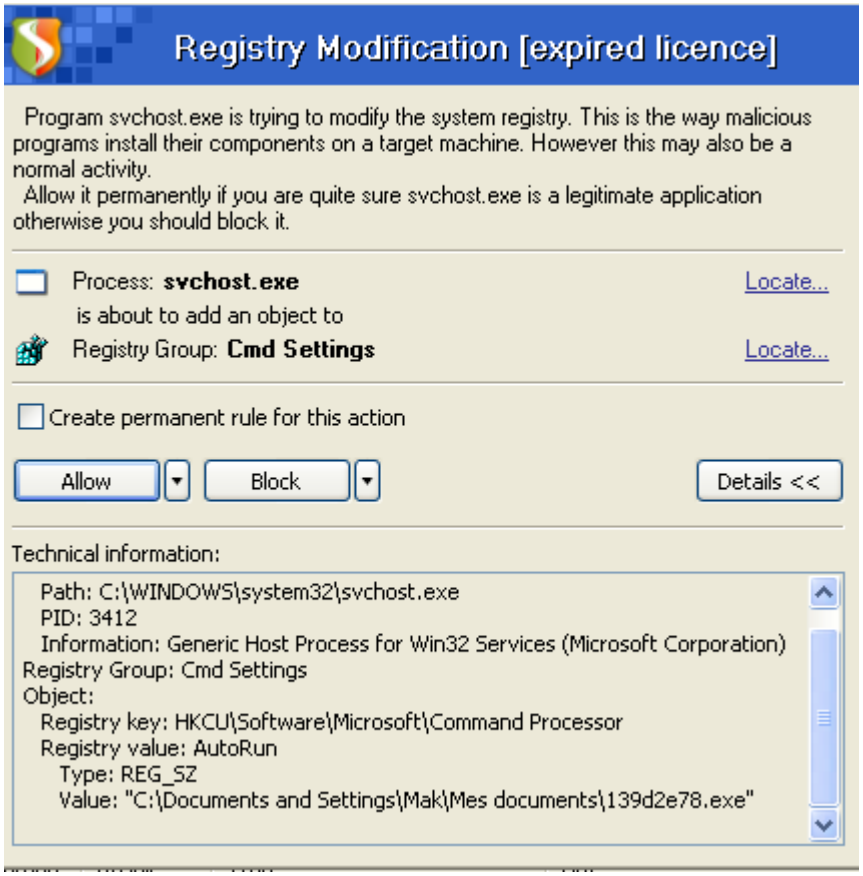
https://www.virustotal.com/fr/file/0671fe7ad24540520202980840 0dad3965ea20dea456b558cee90da098a8538a/analysis/1369477921/

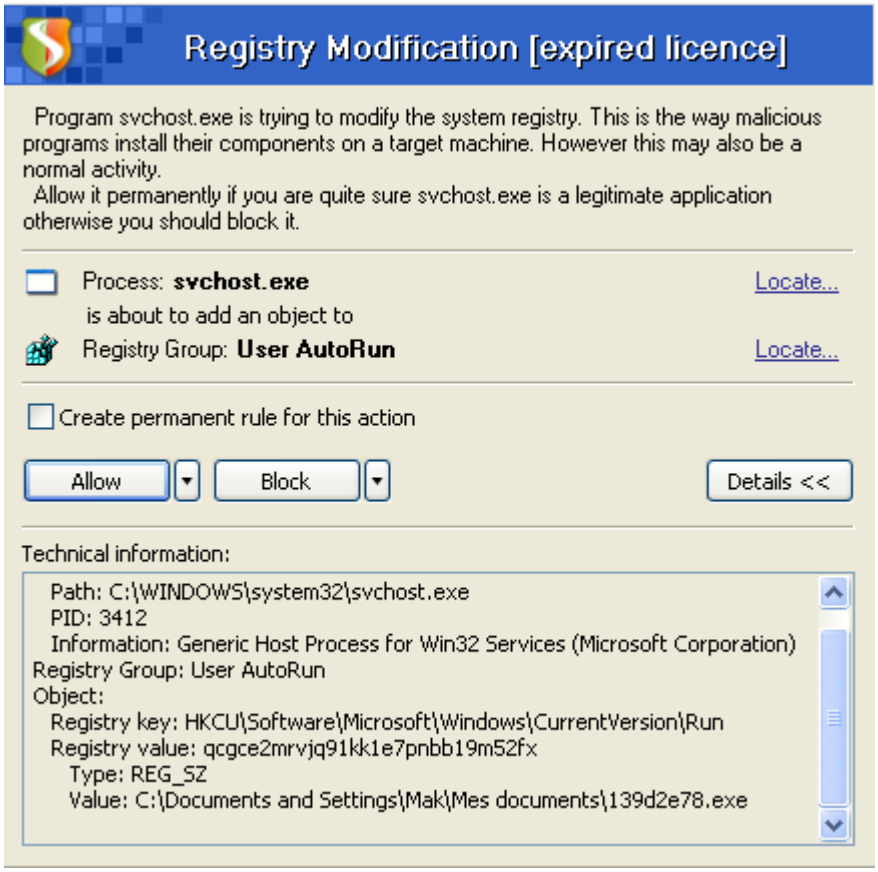
SHA256:
0671fe7ad24540520202980840 0dad3965ea20dea456b558cee90da098a853 8a
Nom du fichier : 3730187.exe
Ratio de détection : 1 / 47
Date d'analyse : 2013-05-25 10:32:01 UTC (il y a 0 minute)

Malwarebytes Trojan.FakeMS 20130525

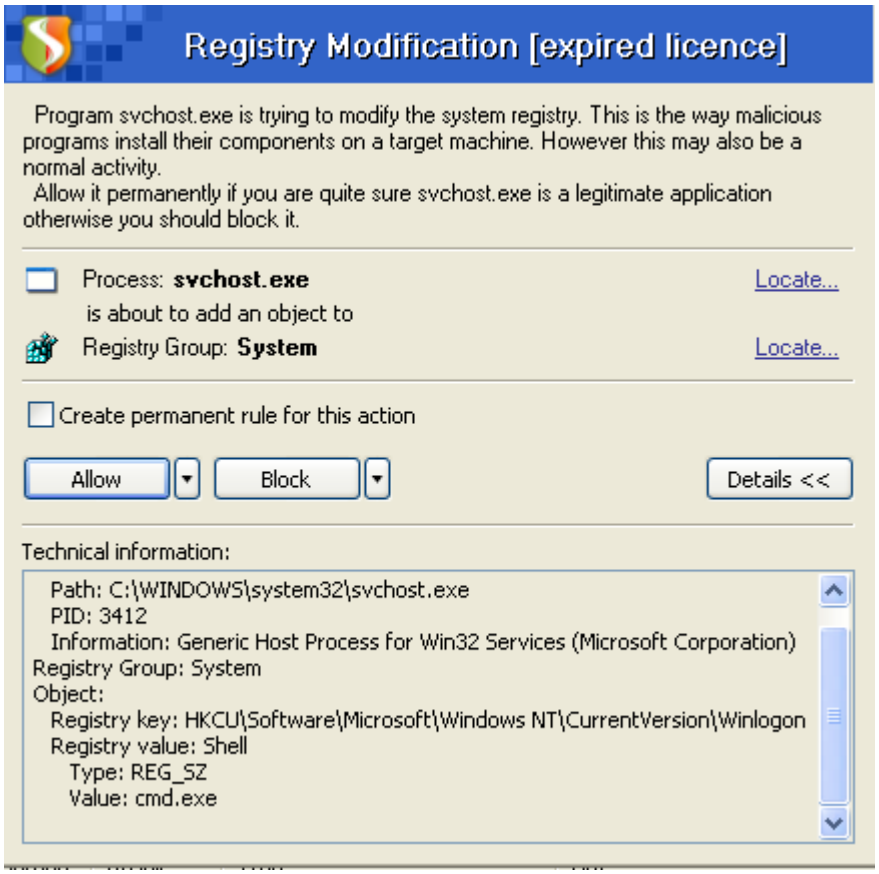


Un fichier dans Mes documents est droppé et la clef Run est créée pour l'utilisateur courant :

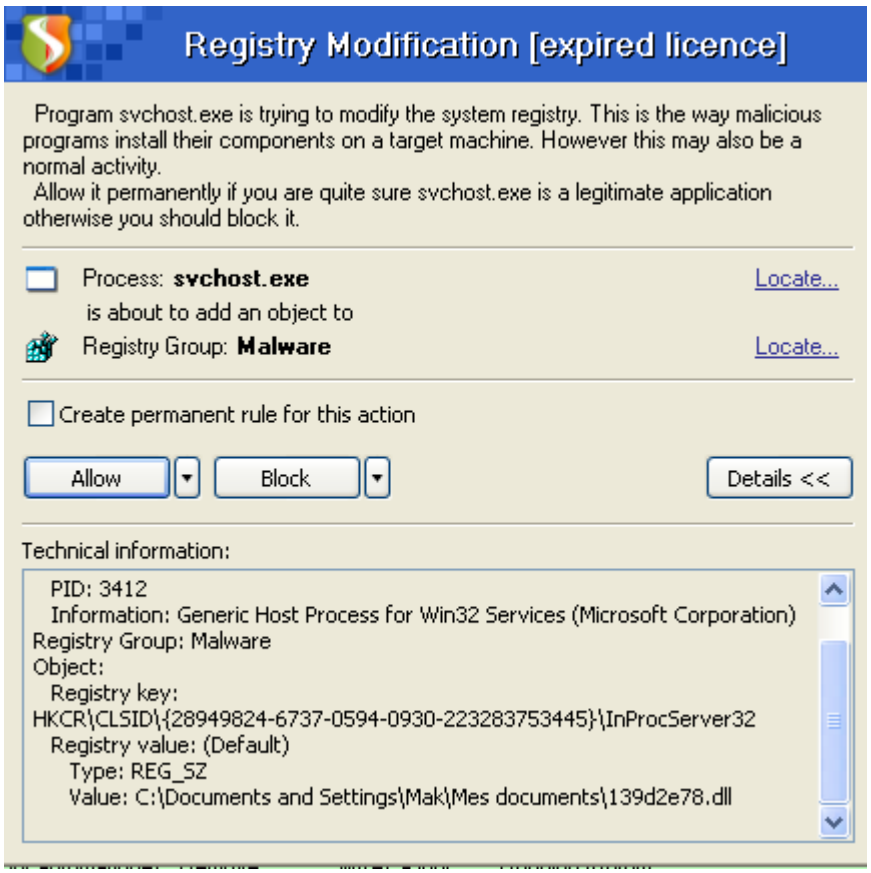




La clef Shell de l’utilisateur courant est modifée vers cmd.exe



Une DLL est aussi droppée et enregistré :



Le malware touche donc une session en particulier.
Si vous avez plusieurs sessions, les autres ne sont pas touchées.

Le malwarare se trouve donc dans le dossier Mes Documents sous forme d'un fichier .exe et .dll aléatoire.

Le .exe :

http://malwaredb.malekal.com/index.php?hash=041550b347da1ded96956701cac7a4c9

https://www.virustotal.com/fr/file/831af342eed7820a4bdfcf893ff431f481bdc032a471aaee8be11c9e4511bedb/analysis/1369475587

SHA256:
831af342eed7820a4bdfcf893ff431f481bdc032a471aaee8be11c9e4511bedb
Nom du fichier : 139d2e78.exe
Ratio de détection : 10 / 47
Date d'analyse : 2013-05-25 09:53:07 UTC (il y a 0 minute)
Avast Win32:Malware-gen 20130525
AVG BackDoor.Generic17.JGS 20130525
Emsisoft Backdoor.Win32.Androm.AMN (A) 20130525
Fortinet W32/Moure.A!tr.dldr 20130525
GData Win32:Malware-gen 20130525
Kaspersky Backdoor.Win32.Androm.rhy 20130525
McAfee Artemis!041550B347DA 20130525
McAfee-GW-Edition Heuristic.BehavesLike.Win32.ModifiedUPX.F 20130525
TheHacker Posible_Worm32 20130524
TrendMicro-HouseCall TROJ_GEN.R47H1EP 20130525

et la DLL :

SHA256:
fb46127aab4102c46324fdc6b01606b131c2e4d00f7e66dda6944a8406432082
Nom du fichier : 139d2e78.dll
Ratio de détection : 6 / 47
Date d'analyse : 2013-05-25 10:29:15 UTC (il y a 0 minute)

AntiVir TR/Crypt.ULPM.Gen2 20130525

AVG BackDoor.Generic17.JGS 20130525
Fortinet W32/Moure.A!tr.dldr 20130525
Kaspersky Backdoor.Win32.Androm.rie 20130525
Panda Suspicious file 20130525
TheHacker Posible_Worm32 20130524

Désinfection

Le malware fait rebooter le PC en mode sans échec sur toutes les sessions.
L'invite de commande est disponible sur les autres sessions que celles infectées.

Restauration du système en invites de commandes en mode sans échec (toutes versions)

Lancer une restauration en invite de commandes en mode sans échec – voir paragraphe Restauration du système en ligne de commandes mode sans échec: https://forum.malekal.com/windows-recuperer-son-systeme-t20428.html#p166263

ATTENTION : Le malware provoque le redémarrage du PC en invites de commandes en mode sans échec sur la session infectée, vous devez choisir une autre session que celle infectée.

Si vous êtes sur Windows Seven, lancer une restauration du système à partir du menu « Réparer mon ordinateur ».
Voir second paragraphe : https://forum.malekal.com/windows-recuperer-son-systeme-t20428.html#p166847

RogueKiller en invites de commandes en mode sans échec (Windows Vista/Seven)

Suivre ce tutorial : https://www.malekal.com/2013/05/30/windows-vistaseven-roguekiller-en-invite-de-commandes-en-mode-sans-echec/

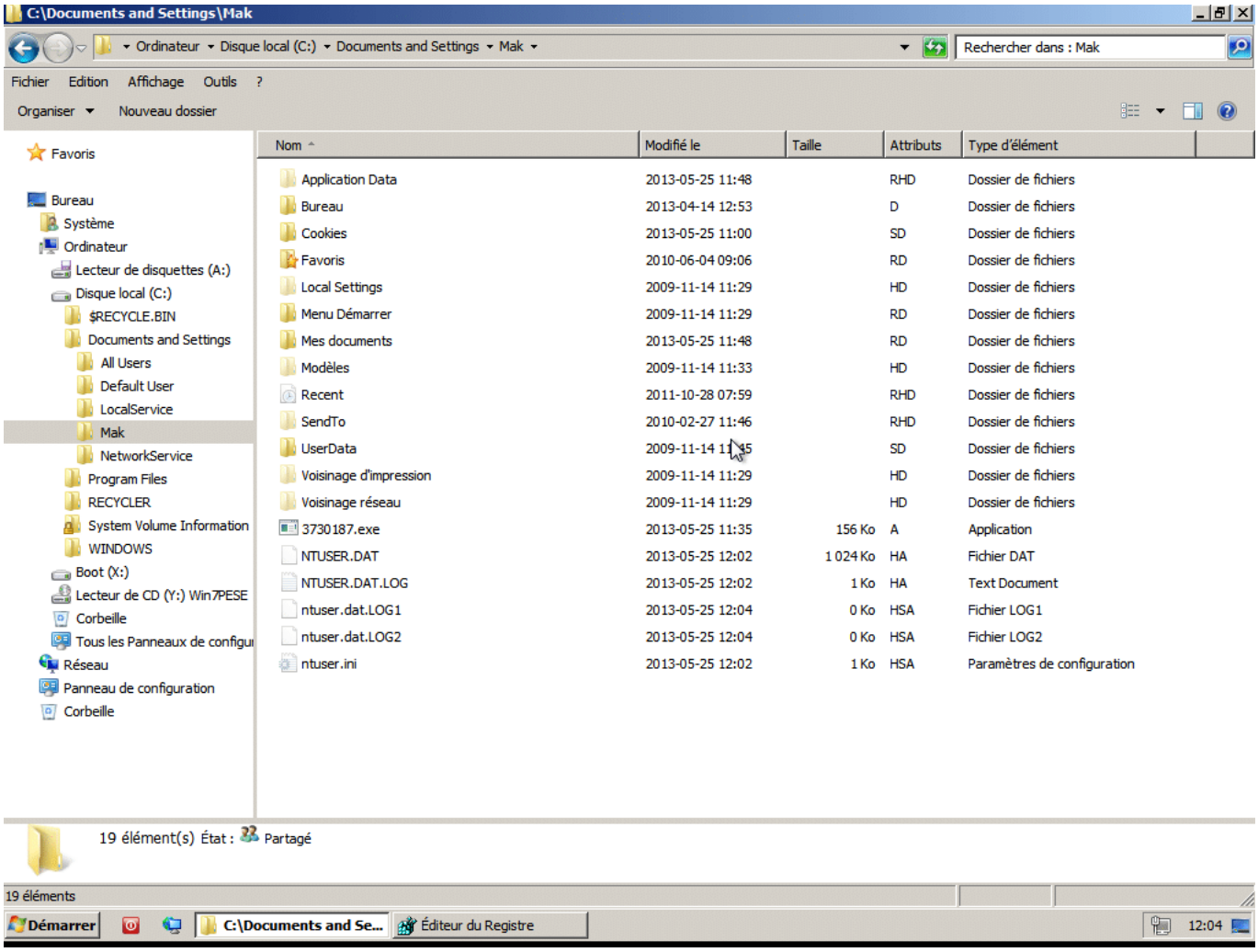
En invite de commandes, s'identifier sur une autre session que celle infectée.

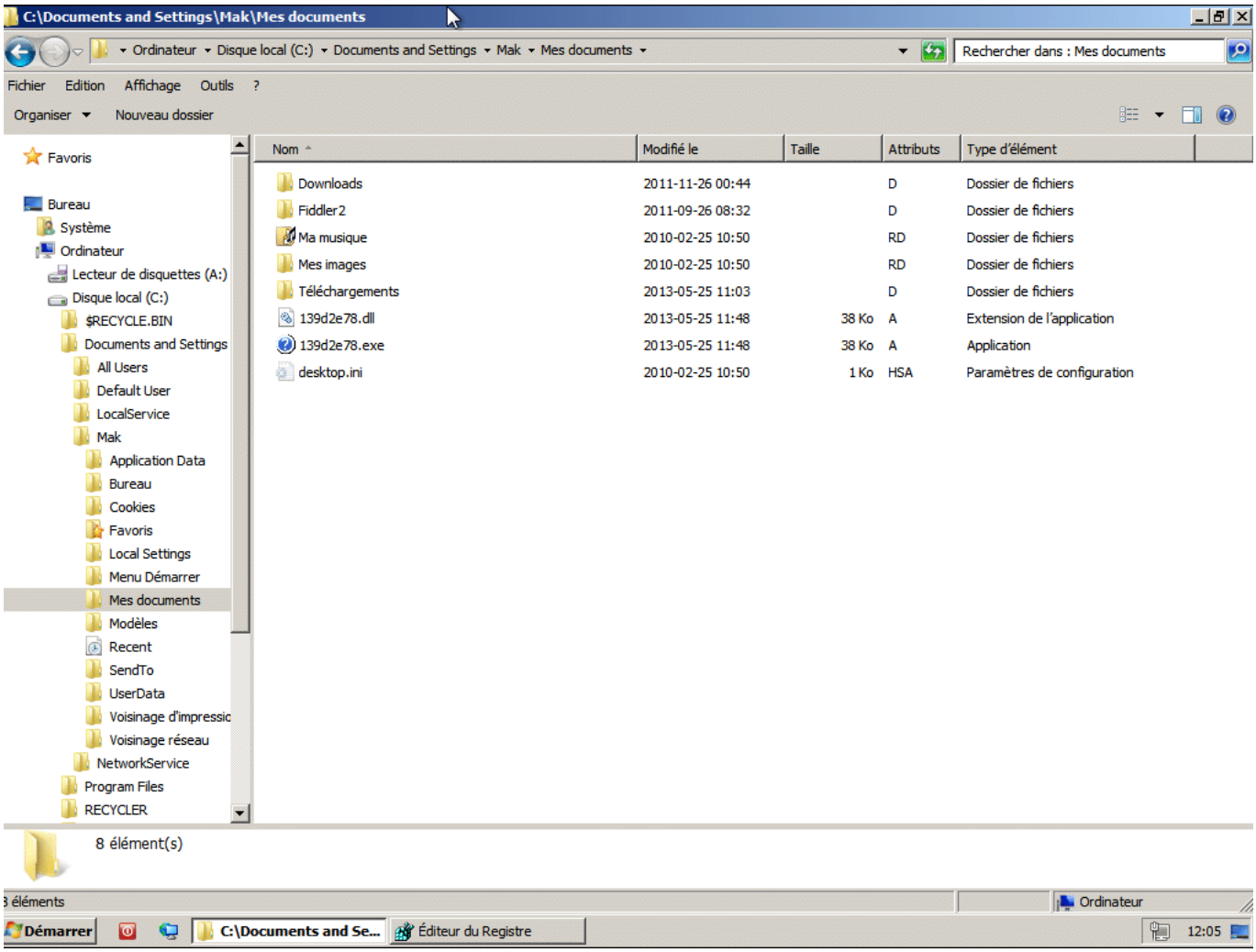
CD Live Malekal

RogueKiller ne gère pas cette variante.

Démarrer le PC infecté sur le CD Live Malekal
Ouvrez mon ordinateur et aller dans le dosser Mes Documents de la session infectée.

Supprimer les deux fichiers .exe et .dll avec les noms aléatoires.


C:\Documents and Settings\Mak
Ordinateur ▸ Disque local (C:) ▸ Documents and Settings ▸ Mak
Rechercher dans : Mak
Fichier Edition Affichage Outils ?
Organiser Nouveau dossier
Favoris
Bureau
Système
Ordinateur
Lecteur de disquettes (A:)
Disque local (C:)
$RECYCLE.BIN
Documents and Settings
All Users
Default User
LocalService
Mak
NetworkService
Program Files
RECYCLER
System Volume Information
WINDOWS
Boot (X:)
Lecteur de CD (Y:) Win7PESE
Corbeille
Tous les Panneaux de configu
Réseau
Panneau de configuration
Corbeille
Nom
Modifié le
Taille
Attributs
Type d'élément
Application Data 2013-05-25 11:48 RHD Dossier de fichiers
Bureau 2013-04-14 12:53 D Dossier de fichiers
Cookies 2013-05-25 11:00 SD Dossier de fichiers
Favoris 2010-06-04 09:06 RD Dossier de fichiers
Local Settings 2009-11-14 11:29 HD Dossier de fichiers
Menu Démarrer 2009-11-14 11:29 RD Dossier de fichiers
Mes documents 2013-05-25 11:48 RD Dossier de fichiers
Modèles 2009-11-14 11:33 HD Dossier de fichiers
Recent 2011-10-28 07:59 RHD Dossier de fichiers
SendTo 2010-02-27 11:46 RHD Dossier de fichiers
UserData 2009-11-14 11:35 SD Dossier de fichiers
Voisinage d'impression 2009-11-14 11:29 HD Dossier de fichiers
Voisinage réseau 2009-11-14 11:29 HD Dossier de fichiers
3730187.exe 2013-05-25 11:35 156 Ko A Application
NTUSER.DAT 2013-05-25 12:02 1 024 Ko HA Fichier DAT
NTUSER.DAT.LOG 2013-05-25 12:02 1 Ko HA Text Document
ntuser.dat.LOG1 2013-05-25 12:04 0 Ko HSA Fichier LOG1
ntuser.dat.LOG2 2013-05-25 12:04 0 Ko HSA Fichier LOG2
ntuser.ini 2013-05-25 12:02 1 Ko HSA Paramètres de configuration
19 élément(s) État : Partagé
19 éléments
Démarrer
C:\Documents and Se...
Éditeur du Registre
12:04



Si vous n'avez aucun fichier, allez dans le dossier Local Settings puis Temp.
Affichez les éléments par liste et cliquez sur la colonne date pour lister les éléments du plus récents au plus anciens.
Si vous avez des fichiers avec des noms aléatoires comme ci-dessus, supprimez le.

Ouvrez le menu Démarrer / System Tools / Registry et Remote Registry

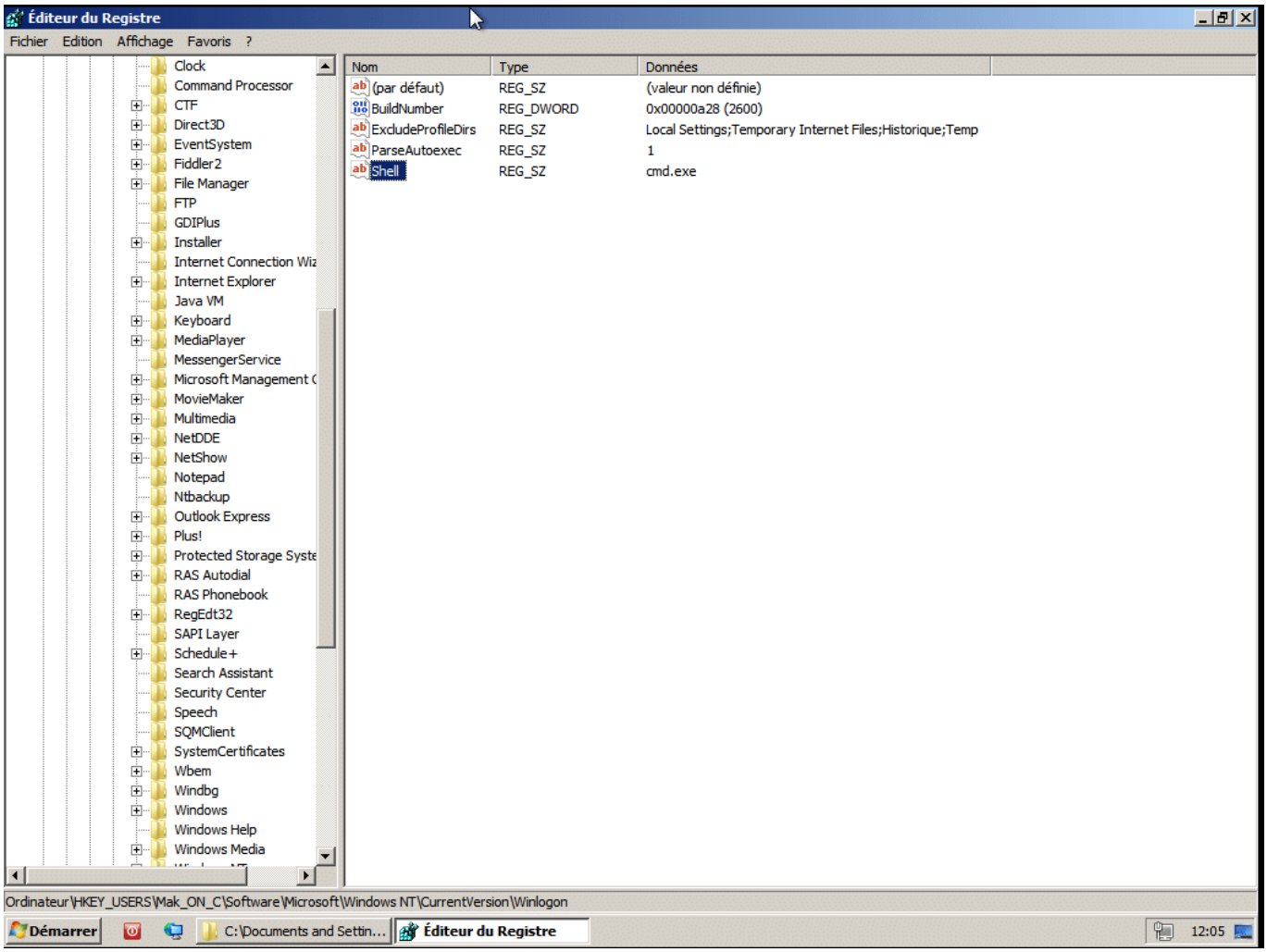
A gauche déroulez l'arborescence suivante :

HKEY_USERS
\SESSIONINFECTEE_ON_C
\SOFTWARE
\Microsoft
\Command Processor
A droite supprimer la clef Autorun.

puis, déroulez ensuite :

HKEY_USERS
\SESSIONINFECTEE_ON_C
\SOFTWARE
\Microsoft
\Windows NT
\CurrentVersion
\Winlogon

A droite, supprimer la clef Shell



Redémarrez l'ordinateur

Après la désinfection – Très important

Changer vos mots de passe WEB (Facebook, Mails, SN, jeux en ligne etc), ces derniers peuvent avoir été récupérés.

Il est ensuite conseillé d'effectuer un scan Malwarebyte => https://www.malekal.com/2010/11/12/tutorial-malwarebyte-anti-malware/

Des PUPs/LPIs sont certainement installés sur votre ordinateur, ces derniers étant très répandus.
Il est conseillé de faire un scan de suppression (bouton suppression) avec AdwCleaner.

Votre ordinateur est vulnérable car vos logiciels ne sont pas à jour – Un site hacké ou une publicité malicieuse qui conduit à un exploit sur site WEB peut infecter votre ordinateur (si votre antivirus est dans le vent, ce qui est souvent le cas).
La source de l'infection est d'avoir sur son ordinateur des logiciels non à jour.
Des logiciels permettent de vous y aider => **https://forum.malekal.com/logiciels-pour-maintenir-ses-programmes-jour-t15960.html**

Pensez à maintenir à jour vos logiciels (notamment Java, Adobe Reader et Flash), ces programmes non à jour permettent l'infection de votre système.
Plus globalement pour sécuriser son ordinateur : Sécuriser son ordinateur (version courte)

Vous pouvez aussi installer HOSTS Anti-PUPs/Adwares qui devrait filtrer les publicités clicksor.

Aucune aide ne sera donnée en commentaire, si vous avez besoin d'aide, créer votre propre sujet sur le forum partie VIRUS : https://forum.malekal.com/virus-aide-malwares-vers-trojans-spywares-hijack.html