sysTPL.exe, société Tlapia et lettre d'avocat

March 31, 2014 • 2 min read • original

Un petit mot sur un programme nommé sysTPL, ce programme a pour but d'évaluer les sites WEB visités.

Pour fonctionner ce dernier installe un proxy (ce qui peux d'ailleurs poser des problèmes de confidentialité => http://forum.malekal.com/anonymisation-sur-internet-avec-proxy-web-t15059.html), une recherche Google montre pas mal de problème de connexion internet dû à la présence de ce proxy.
Dans la majorité des cas, les utilisateurs ne savent pas comment ce programme est venu. Par expérience, je vous dirai que quand la majorité voire la totalité des internautes n'ont  aucune idée comment un logiciel s'est installé sur leurs ordinateurs, ben..... ça pue

Ce WE un webmaster est venu me voir, car il a reçu une lettre provenant d'un avocat qui représente la société Tlapia éditrice du logiciel sysTPL, car le mot malware était utilisé dans un de ces messages..
Il faut savoir aussi que Nicolas Coolman a reçu une lettre du même type car il avait classé ce logiciel comme PUP dans son logiciel ZHPDiag.
Ainsi que d'autres webmasteurs.

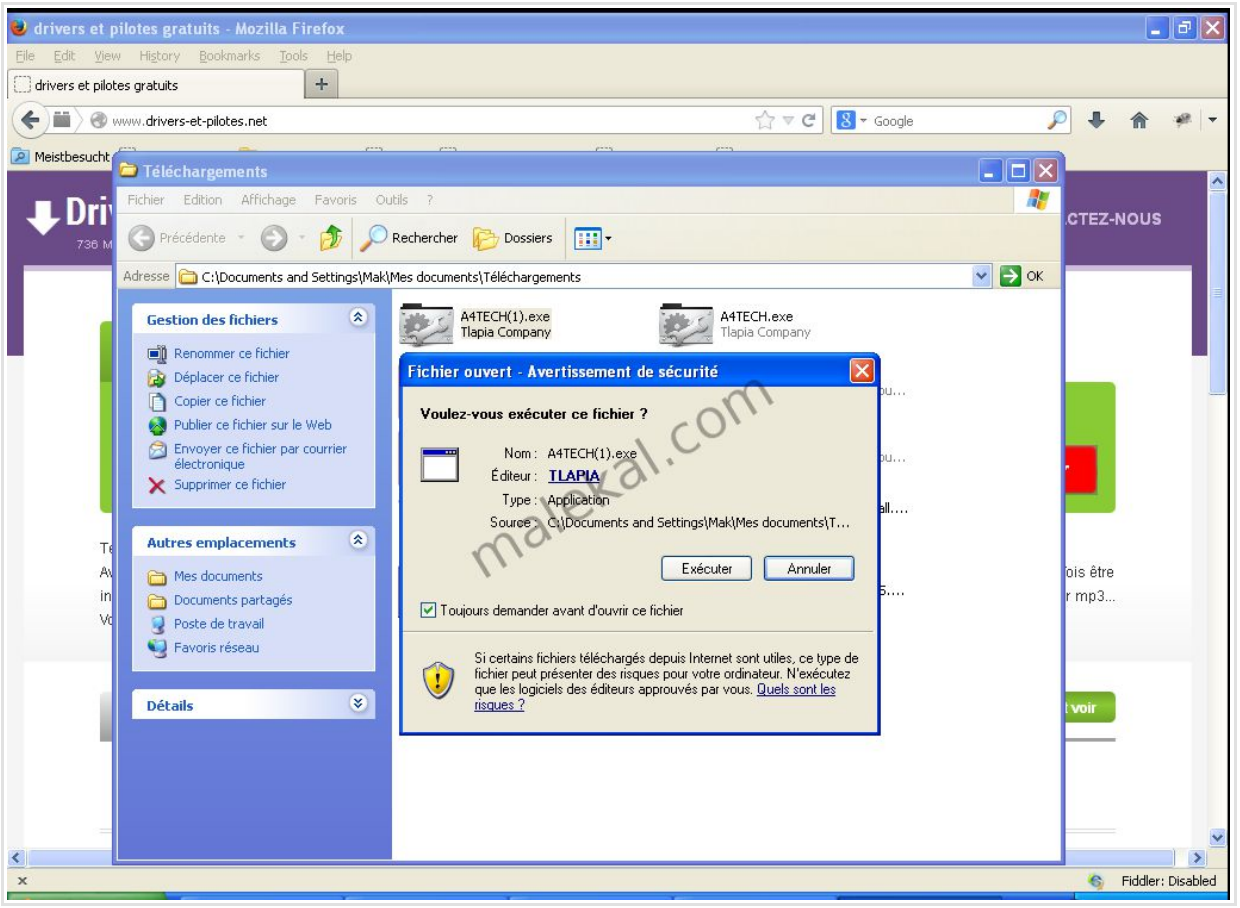
A la base, j'insiste sur le fait que personne ne sait comment ce programme atterrit sur le PC des internautes.
Exemple sur mon forum :
http://forum.malekal.com/proxy-recalcitrant-t44928-15.html
http://forum.malekal.com/systpl-probleme-proxy-sous-chrome-t46630.html
http://forum.malekal.com/probleme-proxy-bis-repetita-t47205.html

J'ai fait une petit recherche là dessus....

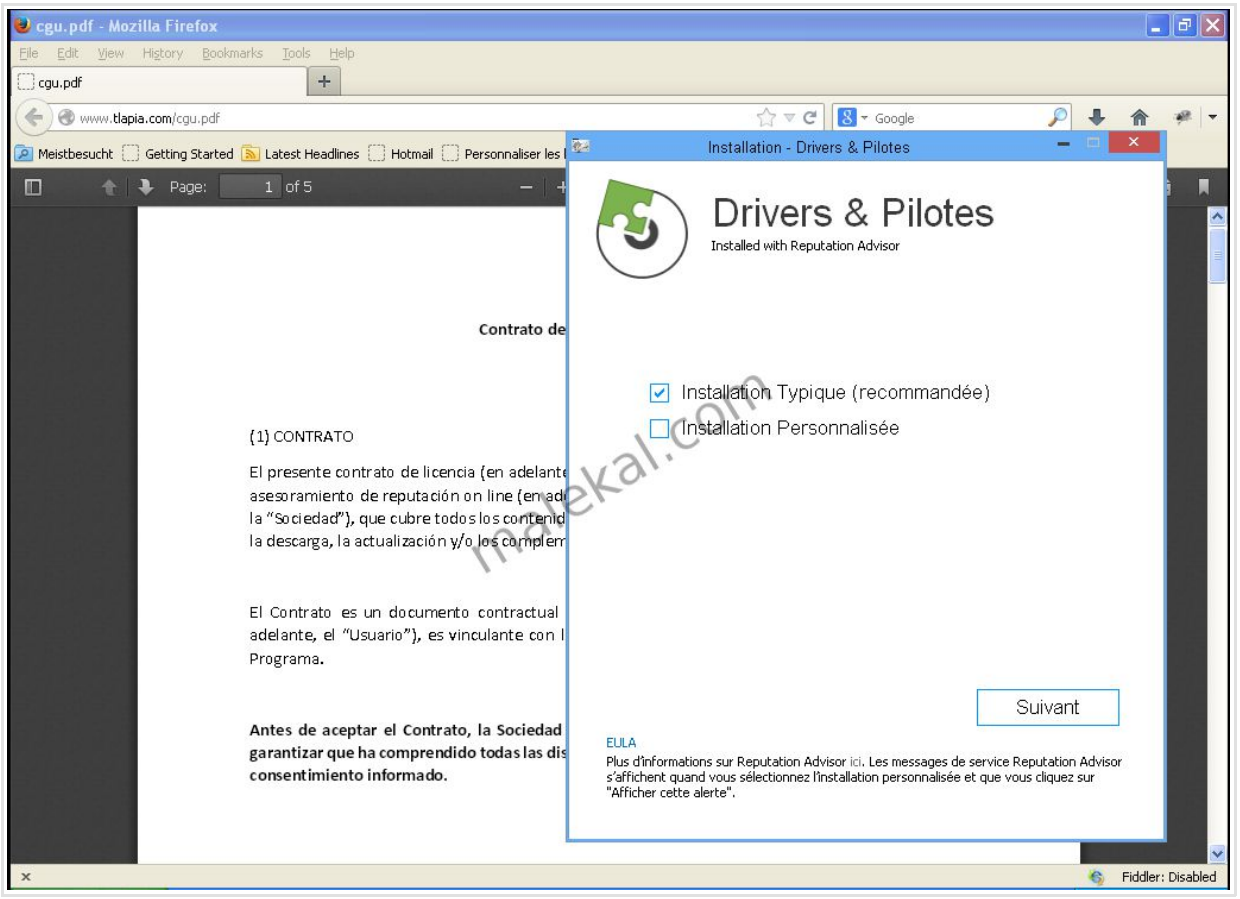
Sur le lien suivant http://www.herdprotect.com/systpl.exe-eb897304ec79e413d89a5dc77453283dc1a99fee.aspx - on constate que le certificat de la signature numérique a été enregistré pour une boîte en Urugay :
CN=TLAPIA, OU=Digital ID Class 3 – Microsoft Software Validation v2, O=TLAPIA, L=Montevideo, S=montevideo, C=UY

Le site www.tlapia.com le confirme :

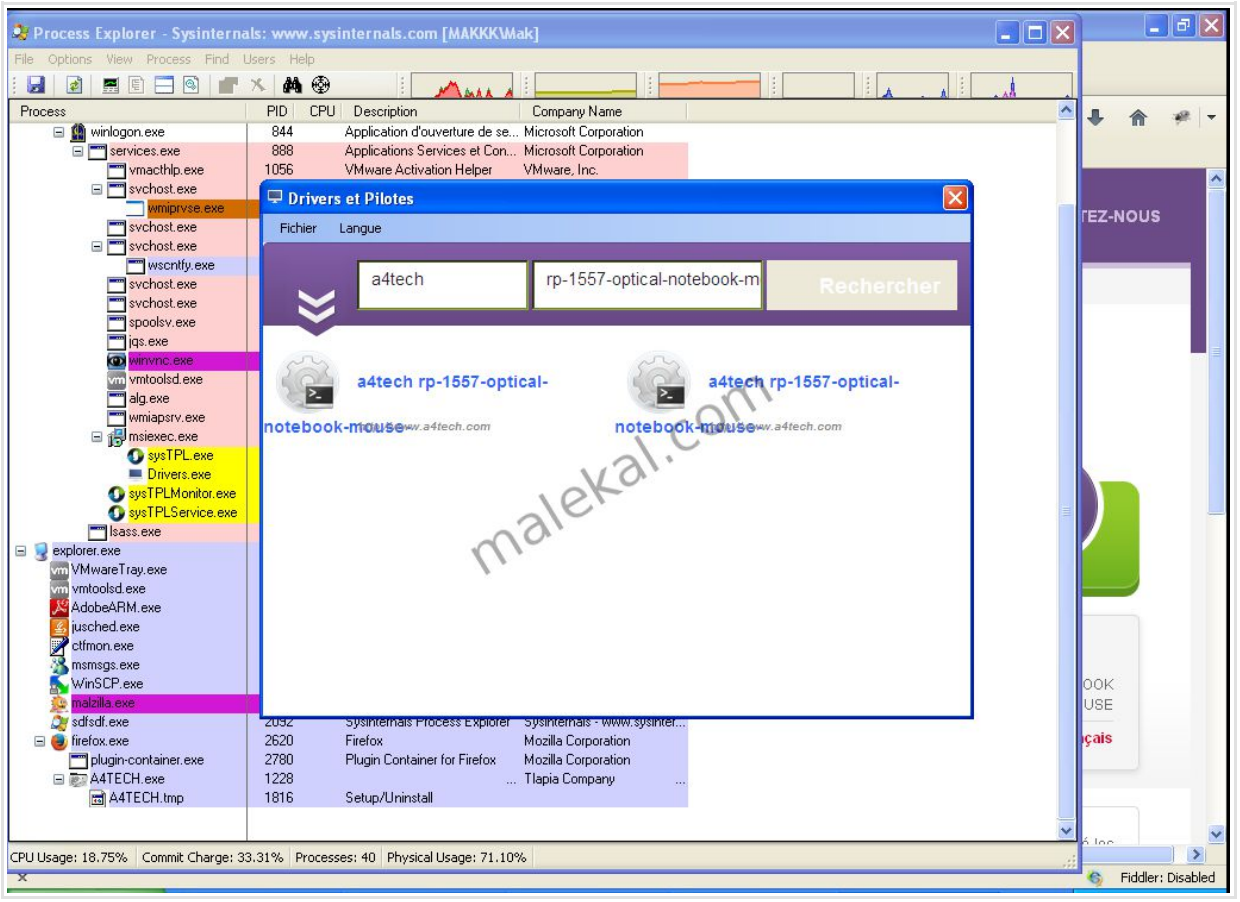
En cherchant un peu, on trouve le site www.drivers-et-pilotes.net – Les fichiers présents là bas sont aussi avec une signature numérique TLAPIA.
Un des fichiers est disponible là : http://malwaredb.malekal.com/index.php?hash=096d9748b5076389a34f0f6acddaf474



Quand on lance, on arrive sur la popup suivante – les conditions d'utilisation sont en Espagnol – humm je ne suis pas sûr que ce soit légal.
Le message EULA est assez incompréhensible.



Et en fait, dès l'ouverture de l'exe, le programme sysTPL s'installe tout seul… soit donc à l'insu de l'utilisateur puisqu'aucun message ne prévient l'utilisateur.
Il ne faut donc pas s'étonner que les internautes crééent des sujets pour des problèmes de proxy ayant pour cause ce programme sysTPL et qu'aucun utilisateur ne soit capable d'expliquer comment il est arriver sur leurs PC.



Compte tenu de ces pratiques, je me suis permis de tagguer le site drivers-et-pilotes.net comme malicieux
: https://www.virustotal.com/fr/url/345aa5a7a1da4627fe77fab4ffa27d1455c3a450876d97

URL:	http://www.drivers-et-pilotes.net/
Ratio de détection :	1 / 52
Date d'analyse :	2014-03-31 15:12:41 UTC (il y a 0 minute)

URL Scanner	
Malekal	Malware site

Quelques autres sites vitrines en langues différentes :
Manuels-et-notices.net
manual-del-usuario.com
support-bedienungsanleitungen.com
support-and-drivers.com
support-und-treiber.com
supporto-e-driver.com

Bref si le programme SysTPL n'est pas malicieux, en ce qui me concerne, il est distribué comme tel (en mode PUP - programmes potentiellements indésirables), je laisse à l'utilisateur l'appréciation sur les pratiques de distribution utilisées.
Est-ce que la définition de malware s'arrête au programme en lui même (ce qu'il fait etc) ou la manière dont l'éditeur ou ses affiliés le distribue ? vaste question, que j'avais abordé dans le sujet : Sur la ligne... : Légitime ou non légitime ? Malware or not malware ?
Personnellement, compte tenu de la poussée des programmes parasites depuis 2/3 ans, il faut prendre en compte la manière dont le programme est distribué dans l'évaluation du programme et non s'arreter au code, le but du programme etc.

Si vous vous retrouvez avec ce programme ou que vous avez des problèmes de connexion/proxy et que cela ne vous intéresse pas de le garder.
Vous pouvez désinstaller SysTPL, pour cela, allez dans programmes et fonctionnalités du panneau de configuration et désinstallez le.
Désactivez les proxys dans tous les navigateurs, voir cette fiche CCM : http://www.commentcamarche.net/faq/28268-desactiver-son-proxy

---

Original URL:
http://www.malekal.com/2014/03/31/systpl-exe-societe-tlapia-et-avocats/