Forum: Généralités

Topic: Dangereux, les logiciels de sécurité informatique ???

Subject: Re: Dangereux, les logiciels de sécurité informatique ???

Publié par: oarsman
Contribution le : 12/05/2016 16:54:14

Citation :

Tof81 a écrit:
Comme d'hab ce genre d'article aguicheur ne donne aucun lien ni référence vers les soit-disant travaux effectués par le professeur adjoint et son doctorant, qui probablement n'a pas encore soutenu sa thèse ...
Je suis bien placé pour savoir qu'en terme de recherche il y du "à boire et à manger".

Tof

PS à Washington : ce n'est pas une critique vis à vis de toi mais des journalistes !

Une histoire de proxy :

Sources :

brève dans TechXplore :
Not so safe: Security software can put computers at risk
http://techxplore.com/news/2016-05-safe-software.html

Article de Xavier de Carné de Carnavalet and Mohammad Mannan
Killed by Proxy:
Analyzing Client-end TLS Interception Software
http://users.encs.concordia.ca/~mmannan/publications/ssl-interception-ndss2016.pdf

Extrait du résumé de l'article (c'est moi qui souligne):
Citation :
—To filter SSL/TLS-protected traffic, some antivirus and parental-control applications interpose a TLS proxy in the middle of the host's communications. We set out to analyze such proxies as there are known problems in other (more matured) TLS processing engines, such as browsers and common TLS libraries. Compared to regular proxies, client-end TLS proxies impose several unique constraints, and must be analyzed for additional attack vectors (...)

Extrait de la conclusion de l'article:
Citation :
we found that not a single TLS proxy implementation is secure with respect to all of our tests, sometimes leading to trivial server impersonation under an active man-in-the-middle attack, as soon as the product is installed on a system. Our analysis calls the purpose of such proxies into question, especially in the case of antiviruses, which are tasked to enhance host security. Indeed, these products in general, appear to significantly undermine the benefits of recent security fixes and improvements as deployed in the browser/SSL ecosystem. We suggest preliminary guidelines for

safer implementations of TLS proxies based on our findings.
However, due to the foreseeable implementation complexities of our proposed guidelines, we suggest the adoption of interfaces that would let client-end TLS proxies monitor encrypted traffic originating from browsers in a more secure way, e.g., using the SSL key log file feature. Our work is intended to highlight weaknesses in current TLS proxies, and to motivate better proposals for safe filtering. Finally, our findings also call into question the so-called security bestpractice of using antiviruses on client systems, as commonly advised by IT professionals, and even required by some online banking websites.

J'oubliais le lien vers la page de l'auteur thésard:
https://madiba.encs.concordia.ca/~x_decarn/