"Téléchargez moi" – Dire Oui
est le terme le plus dangereux du Web

There's no such thing as a free lunch. " Il n'y a rien de vraiment gratuit".

Cette présentation est extraite de l'article :
Download me—Saying “yes” to the Web’s most dangerous search terms

Le Principe

À l'image du film "Super-Size Me" nous allons voir ce qui se passe lorsque que nous surfons avec le gratuit.

- Une seule directive dire oui à tout et constater.
- La machine est équipée de :
  - Mozilla Firefox avec Surf en anonyme
  - Microsoft Security Essentials
  - Lavasoft's Ad-Aware.

Étude - Les mots recherchés les plus dangereux du Web

"free e-cards," listed in the McAfee Top 50, US

"free game cheats," “game cheats” qualifies as a McAfee Top 50

"free games," noted as popular generic search query

"free lyrics," “lyrics," and “song lyrics” were among the McAfee Top 50

"free music downloads," the No. 1 term for Average Risk, McAfee Top 50

"free screensaver," noted as a popular generic search query

"free wallpaper," “wallpaper” is a McAfee Top 50

"free word unscrambler," the No. 1 term for Maximum Risk, McAfee Top 50

Dans le rapport de Mc Affee,

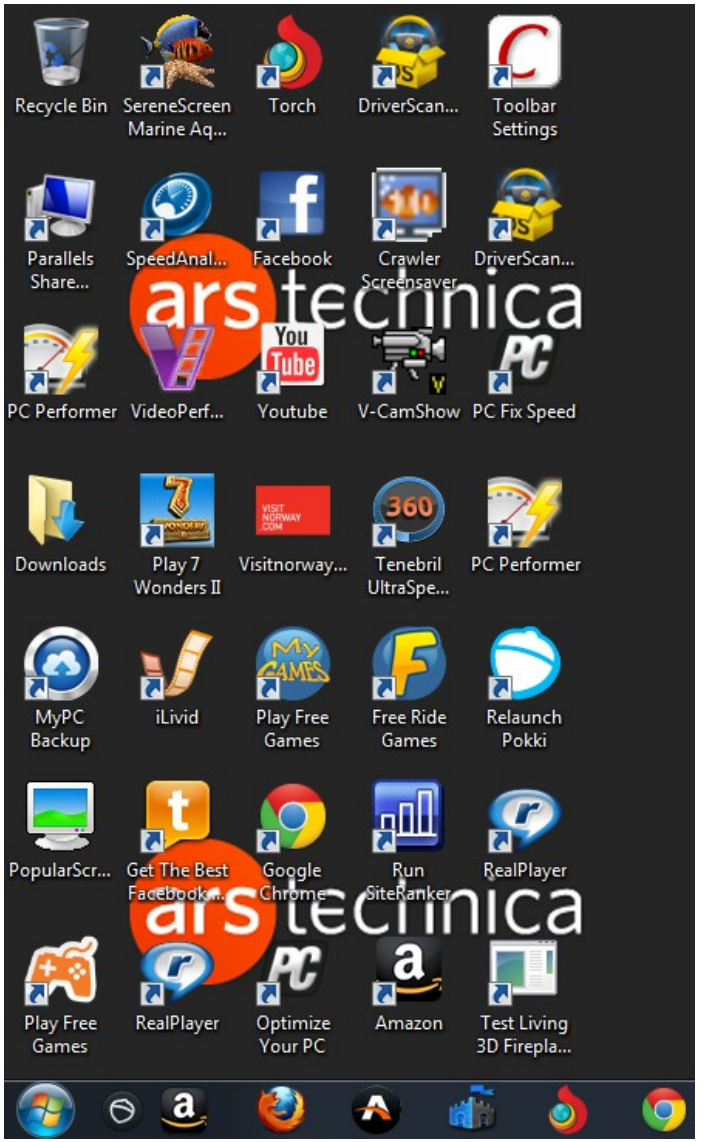
"free" a la catégorie de risques la plus élevée

Gratuit - "free wallpaper" and "free screensaver"

Des aides au téléchargement sont proposées avec les logiciels, parmi celles-ci : http://www.ilivid.com/

Le nombre d'icônes présentes sur le bureau passe **de 3 à 35** et de nouveaux composants additionnels viennent se greffer à Mozilla.

Internet : l'essence de vie des AdWares



Gratuit - "free games"

Free Games

Le trojan Yontoo fait son apparition au travers des jeux :

- ***Mahjong World* and the Free Ride**
- ***Treasures of Montezuma 3***

Le malware Ask malware toolbar et l'application Weather Channel App s'installe avec le jeu ***SafariGames***

Free games cheats (code pour progresser)

EZGameCheats s'accompagne de l'installation de InstallIQ.

- InstallIQ procure des mécanismes tierces pour "offrir" des composants additionnels.

Bilan - "free wallpaper"

L'installation de fonds d'écran gratuits a conduit à l'installation de :

- **2 plugins Firefox:** Fun Web Products Plugin Stub 1.0.1.0, MindSpark Toolbar Platform Plugin Stub 1.0.1.1
- **4 extensions Firefox:** MapsGalaxy 1.2, MapsGalaxy 2.73.1.10084, Marine Aquarium Lite 2.73.1.2046, Yontoo 1.20.02
- **9 programmes complets téléchargés.**

Bilan - "free screensaver" (1/2)

L'installation d'économiseurs d'écran gratuits a conduit à l'installation de :

- **10 plugins Firefox :** Exent AOD Gecko Plugin 7.0.0.3, GameTreatWidget 8.1.57.0, Google Update 1.1.21.145, RealDownloader Plugin 1.3.1.2, RealNetworks((TM)) RealDownloader Chrome Background Extension Plug-In (32-bit), RealNetworks((TM)) RealDownloader HTML5VideoShim Plug-In (32-bit) 1.1.1.2, RealNetworks((TM)) RealDownloader PepperFlashVideoShim Plug-In (32-bit) 1.1.1.2, RealPlayer Download Plugin 16.0.1.18, RealPlayer((TM)) G2 LiveConnect-Enabled Plug-In (32-bit) 16.0.1.18, Shockwave Flash 11.7.700.169
- **13 extensions Firefox :** Amazon Browser Bar 3.0.20121130, Crawler Toolbar 1.7.11, getsav-in 5.0, MapsGalaxy 2.73.1.10084, Marine Aquarium Lite 2.73.1.2046, SavetheChildrenApp By We-Care.com 4.1.20.1, SearchDonkey 2.5.91, SiteRanker 1.0.0.1, SweetPacks Toolbar for Firefox 1.13.0.1, Updater By SweetPacks 2.0.0.566, Yontoo 1.20.02

Bilan - "free screensaver" (2/2)

L'installation d'économiseurs d'écran gratuits a conduit à l'installation de :

- **27 programmes téléchargés :** Amazon App (shortcut), Crawler Screensaver, Crawler Toolbar, UniBlue DriverScanner, Get The Best Facebook Chat Messenger (shortcut), Google Chrome, iLivid, InstallIQ, MyPC Backup, Optimize Your PC, PC Fix Speed, PC Performer, Play 7 Wonders II (Free Ride Games), Play Free Games (shortcut), RealPlayer, Pokki, Run SiteRanker, SereneScreen Marine Aquarium Lite, SpeedAnalysis, Tenebril UltraSpeed 360, Virdi Software V-Cam Show v1.5.2, Test Living 3D Fireplace 2.0, Torch (a torrenting Web browser that looks like a Chrome clone), Visitnorway_Norway Tourism Screensaver, YouTube (shortcut), SohoScreens, Wajam

Bilan - "free games"

L'installation de jeux gratuits a conduit à l'installation de :

- **4 plugins Firefox :** Extent AOD Gecko Plugin 7.0.0.3, GameTreatWidget 8.1.57.0, Google Update 1.3.21.145, Shockwave Flash 11.7.700.169
- **7 extensionsFirefox :** Arcadesafari 2.3.796, Ask Toolbar 12.40906, RapidFinda 1.0, SweetPacks Toolbar for Firefox 1.13.0.1, Tidy Network 4.0, Updater by SweetPacks 2.0.0.566, Yontoo 1.20.02
- **14 programs téléchargés :** Mario Forever!, Mario Info!, Solitaire Haven, The Weather Channel App, Play Free Games (Free Ride Games), More FREE Games (Free Ride Games), The Treasures of Montezuma 3 (Free Ride Games), Mahjong World (Free Ride Games), EXETender Player (for Treasures of Montezuma), Google Drive, Google Chrome, Adobe Flash, RapidFinda, Arcadesafari

Bilan - "free games cheats"

L'installation de cheats a conduit à l'installation de :

- **5 plugins Firefox :** MapsGalaxy 2.73.1.10084, SavetheChildren App By We-Care.com 4.1.20.1, SearchDonkey 2.6.14, Yahoo Toolbar 2.5.7.20130322105505, Yontoo 1.20.02
- **2 Extensions Firefox :** MindSpark Toolbar Platform Plugin Stub 1.0.1.1, Shockwave Flash 11.7.700.169
- **3 Programmes Téléchargés :** EZ Game Cheats, Weatherbug, Adobe Flash

Conclusion

Lorsque vous exécutez un logiciel **à partir d'une source "non-sûre"**, le logiciel envoie des informations au sujet de votre système d'exploitation au "fabriquant" du logiciel, informations telles que :

- le modèle de votre ordinateur
- votre adresse IP
- vos programmes
- votre navigateur

Et, si en plus, vous avez installé un logiciel pilier de l'AdWare, révéler ces informations n'est pas sain, vos informations seront en effet alors transmises directement sur le serveur d'AdWare et votre adresse IP ou un élément d'identification de votre ordinateur sera associé à

Un utilisateur "crédule" …

Pour aller plus loin

http://www.youtube.com/watch?v=TgaZDNgxfQQ

DEFCON 18: My Life as a Spyware Developer