Analyse du logiciel "SiteAdvisor" de McAfee

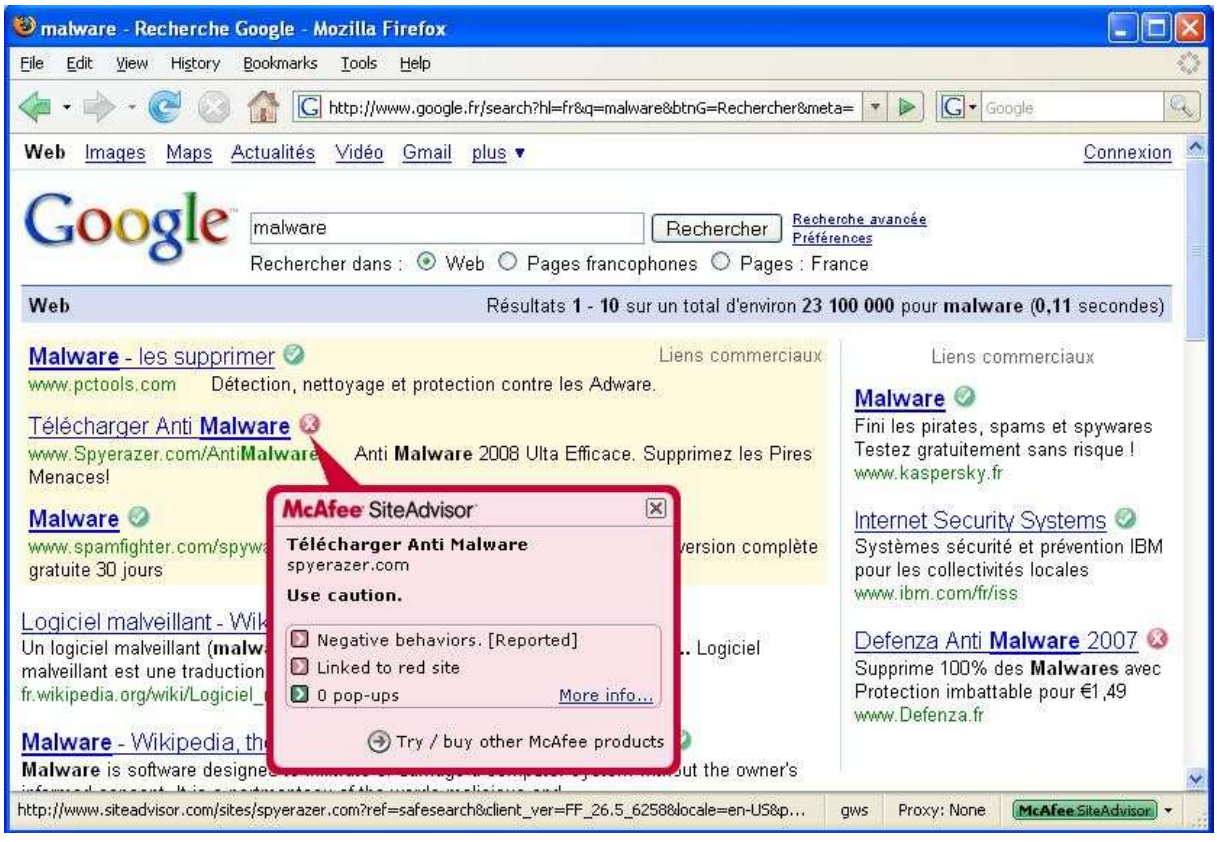
L'un de nos adhérents nous a consultés pour avoir notre avis sur le logiciel "SiteAdvisor" de McAfee (www.siteadvisor.com). Dans ce cadre, nous avons réalisé une mini-étude de ce produit, et nous vous en présentons les résultats.

Présentation de SiteAdvisor

SiteAdvisor est un produit gratuit qui s'intègre aux navigateurs web Firefox et Internet Explorer et qui a pour objectif de rendre la navigation web sur Internet plus sure.

Il existe aussi une version payante du produit, baptisé "SiteAdvisor Plus", qui étend les fonctionnalités de base de la version gratuite. Celle-ci prend également en compte les e-mails et les outils de messagerie instantanées, et donne la possibilité d'interdire la visite des sites web jugés non surs. Cette version payante n'a pas été étudiée.

Pour ce faire, lorsque l'internaute utilise un des moteurs de recherche connus de SiteAdvisor (par exemple Google, YahooSearch ou LiveSearch), une signalétique est automatiquement ajoutée par SiteAdvisor dans le résultat de la recherche pour indiquer la dangerosité des sites affichés (voir image ci-dessous).



Cette signalétique est la suivante :

- un macaron vert indique un site sûr,
- un macaron rouge un site dangereux,
- un macaron jaune un site plutôt suspect,
- Un macaron gris un site inconnu (auquel aucune note n'a été attribuée par SiteAdvisor).

SiteAdvisor indique également en permanence en bas à droite du navigateur la dangerosité du site web courant. Dans l'exemple ci-dessus, le bouton vert "McAfee SiteAdvisor" indique que le site courant (www.google.fr) est jugé sûr.

Fonctionnement technique de SiteAdvisor

Afin de mieux comprendre le fonctionnement de SiteAdvisor et de connaitre les informations que ce logiciel envoie vers son site web de référence (site contenant la base de donnée des notations pour chaque site web visité), nous avons observé au cours d'une campagne de tests, les échanges réseaux produits par le plug-in SiteAdvisor pour Firefox.

Lors de ces tests nous avons observé 3 types de requêtes générées par SiteAdvisor :

- La requête "**Ping**" teste la connectivité réseau.
- La requête "**Query**" demande la notation pour un site.
- La requête "**MultiQuery**" demande la notation pour un ensemble de sites.

Nous décrivons en détails ces requêtes ci-dessous. Globalement, le comportement observé est conforme à ce que l'on pouvait s'attendre, ce qui est rassurant.

Requête "Ping" :

Exemple de requête "Ping" observée lors des tests :

```
GET https://dss1.siteadvisor.com/DSS/Ping?includeVersionInfo=true&version=2
&client_ver=FF_26.5_6254&locale=en-US&aff_id=0
&UID=b45c0b2a-6e13-44f9-b841-75e68d171c61 HTTP/1.1
```

Visible, cette requête sert à vérifier la version du Plugin SiteAdvisor, mais permet aussi de récupérer des données sur le poste client : version de Firefox, Identification de l'utilisateur (UID).

La réponse retournée par le site web "siteadvisor.com" est moins compréhensible. En voici un exemple :

```
<PingResponse>
<VersionInfos><VersionInfoArray>

<VersionInfo entity="ClientExe" version="2.6.0.6253"
cksum="d6837e67ff23d2236b9016d140864151"
location="sadownload.mcafee.com/products/SA/IE/upgrade/0/saSetup.exe"
immediate="false"/>

<VersionInfo entity="ClientSupport" version="2.6.0.6254"
cksum="f79b6762425e1e08d1173e7bf98a1c98"
location="sadownload.mcafee.com/products/SA/IE/upgrade/0/SiteAdv.pak"
immediate="false"/>

<VersionInfo entity="search.dat" version="6254" cksum="0123456789ABCDEF"
location="https://sadownload.mcafee.com/products/sa/firefox/search.dat" immediate="false"/>

</VersionInfoArray></VersionInfos>
</PingResponse>
```

Visiblement cette réponse contient des URLs (paramètres "location" ci-dessus) vers des données téléchargeables. D'après le nom des chemins d'accès, il s'agirait de données permettant de mettre à jour SiteAdvisor dans des environnements Internet Explorer ou Firefox. Une analyse plus approfondie des fichiers "SiteAdv.pak" et " search.dat" (ils contiennent tous deux du code Javascript) pourraient être cependant intéressante pour mieux comprendre le fonctionnement du produit.

Requête "Query" :

Exemple de requête "Query" observée lors des tests :

```
GET http://dss2.siteadvisor.com/DSS/Query?Entitlement=FOO&Type=domain&version=2
&name=www.crackz.ws&client_ver=FF_26.5_6254&locale=en-US&aff_id=0 HTTP/1.1
```

Cette requête "Query" a été générée par SiteAdvisor pour interroger la base de données SiteAdvisor à propos du site www.crackz.ws.

Voici la réponse reçue pour cette requête :

```
<DomainQueryResponse>
<DomainInfo name="crackz.ws" expires="1203255903" popularity="LESS_POPULAR">
<DomainMetaData baseDomain="crackz.ws" dateCreated="0" isDynamicIP="false"
isUserContent="false" domainSpecRegExs="^{[^/\\]+\.}*(crackz\.ws){[:/\\?].*}$">
<Location country="NL" state="" city=""/>
</DomainMetaData>

<Classification code="WARN" color="red">
<description>Feedback from credible users suggests that downloads on this site may contain
what some people would consider adware, spyware, or other potentially unwanted
programs.</description>
</Classification>

<FacetInfos>
<CommerceInfo code="UNKNOWN"><description/><short_desc/></CommerceInfo>

<DownloadsInfo code="WARN"><description>Feedback from credible users suggests that
downloads on this site may contain what some people would consider adware, spyware, or
other potentially unwanted programs.</description><short_desc>Risky downloads
[Reported]</short_desc></DownloadsInfo>

<PersonalInformationInfo code="UNKNOWN"><description>We have not found any e-mail
sign-up forms on this site.</description><short_desc>0 sign-up forms
found</short_desc></PersonalInformationInfo>

<AnnoyanceInfo code="OK"><description>When we browsed this site we received a few
pop-ups.</description><short_desc>1 pop-up</short_desc></AnnoyanceInfo>

<LinksInfo code="WARN"><description>When we tested this site we found links to andr.net,
which we found to be a distributor of downloads some people consider adware, spyware or
other potentially unwanted programs.</description><short_desc>Linked to red
sites</short_desc></LinksInfo>

<RogueInfo code="UNKNOWN"><description/><short_desc/></RogueInfo>
</FacetInfos>
</DomainInfo>
</DomainQueryResponse>
```

Cette réponse est assez lisible. On y voit que le site web est basé en hollande (**Location country="NL**"), et que sa notation globale va être rouge (**Classification code="WARN" color="red")**. On trouve ensuite le détail de ce jugement : Peut-on télécharger des choses dangereuses de ce site ? Peut-on se faire voler des informations personnelles sur le site, etc…

Requête "MultiQuery" :

La requête "MultiQuery" est équivalente à une requête "Query", sauf que cette fois on interroge la base SiteAdvisor à propos d'un ensemble de site.

Voici un exemple de requête "MultiQuery" capturée :

> POST http://dss2.siteadvisor.com/DSS/MultiQuery HTTP/1.1
> Entitlement=FOO&Type=domain&version=2&client_ver=FF_26.5_6254&locale=en-US&aff_id=0&**Name_1=**www.crackz.ws&**Name_2=**sbrousseau.free.fr&**Name_3=**www.appzplanet.com&Name_4=mts.free.fr&Name_5=www.subserials.net&Name_6=www.commentcamarche.net&Name_7=mathos.mylinea.com&Name_8=creative.com.net.online.fr&Name_9=forum.hardware.fr&Name_10=www.sospc-en-ligne.com&count=10

On y voit ici que l'on interroge la base SiteAdvisor à propos de dix sites web : paramètres Name_1 à Name_10.

Le résultat obtenu pour chacun des dix sites est équivalent à celui que nous avons présenté pour la requête "Query".

Analyse de points particuliers

McAfee peut-il espionner mon activité lorsque j'utilise SiteAdvisor ?

On peut redouter que les informations renvoyées par le plug-in "SiteAdvisor" vers le site web "siteadvisor.com" permette d'espionner l'internaute.

Cela est vrai en partie, car on a vu lors de l'analyse technique que le nom des sites visités (ou recherchés sous Google) sont systématiquement envoyés vers le site "SiteAdvisor.com".

Par contre les informations envoyées sont très limitées :

- seul le nom du site (par exemple www.microsoft.com) est envoyé, et non l'URL en entier (par exemple www.microsoft.com/technology/mobility/item).
- de plus les paramètres éventuellement utilisés pour les sites visités par l'internaute (par exemple nom d'un compte ou mot de passe) ne sont pas inclus dans les données envoyées à "SiteAdvisor.com".

L'information recueillie reste donc limitée.

Nota : Il aurait été possible à SiteAdvisor de diminuer l'information recueillie en envoyant l'empreinte MD5 correspondant au site visité, plutôt que son nom en clair. Dans le cas ou ce site n'est pas déjà connu de SiteAdvisor, ce dernier n'a alors pas de moyen de savoir de quel site il s'agit, ce qui limite l'information recueillie. Cela aurait cependant aussi un effet négatif puisque SiteAdvisor ne pourrait alors pas savoir les nouveaux sites web qu'il doit ajouter à ses campagnes de tests et de notation.

La politique d'utilisation des données collectées par SiteAdvisor

SiteAdvisor indique dans sa charte d'utilisation qu'il collecte des données à propos de l'utilisation de SiteAdvisor, mais que ces données sont anonymes (elles ne sont pas associées à un utilisateur identifiable) et n'existe que pour les personnes ayant accepté de participer au programme "PIP" (Product Improvement Program).

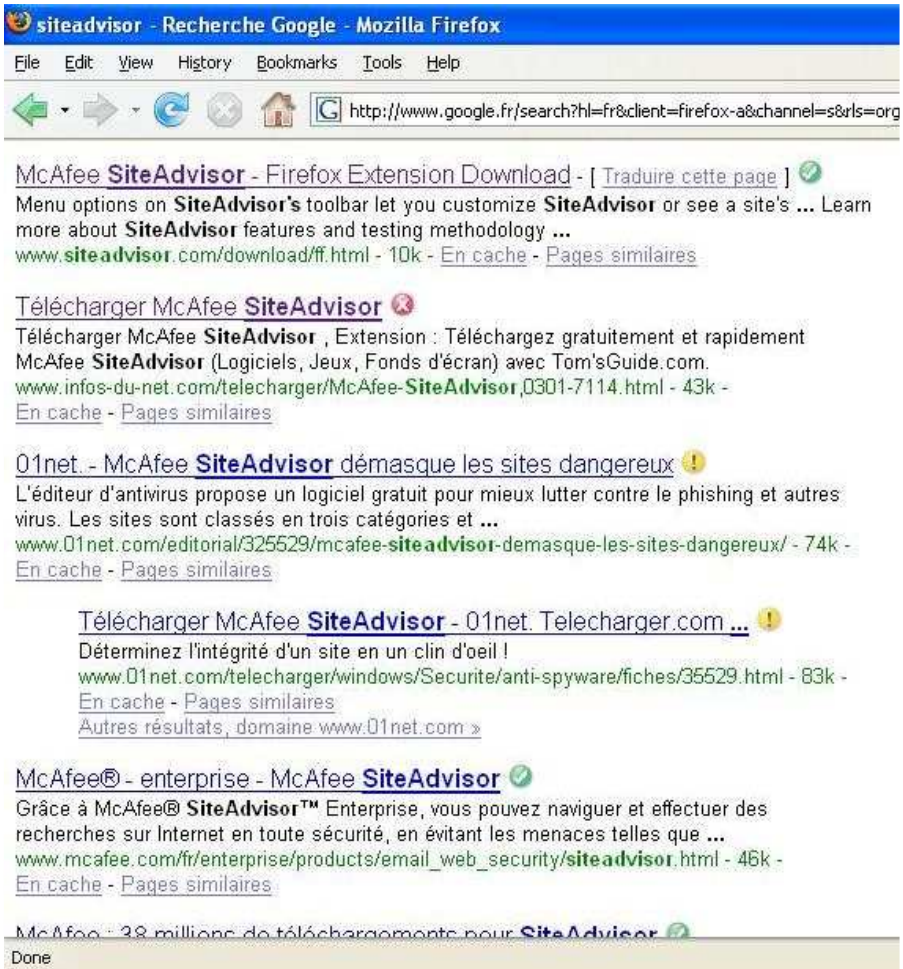
En septembre 2007, SiteAdvisor a annoncé cependant qu'il assouplissait sa charte en s'autorisant désormais à transmettre les données anonymes collectées à des "Partenaires"(cf. l'annonce http://blog.siteadvisor.com/2007/09/change_to_our_privacy_policy.shtml).

Les termes de la charte d'utilisation paraissent globalement raisonnables, mais l'assouplissement observé et la cession de ces données à des tiers non identifiés est tout de même un fait inquiétant.

Efficacité du produit

Lors de nos tests, nous avons observé quelques résultats surprenants.
Par exemple, les sites français suivants sont classés comme suspects par SiteAdvisor (voir image) :

- www.infos-du-net.com est classé "rouge" parce que SiteAdvisor indique qu'il a téléchargé sur ce site deux programmes qui se sont révélés être des "malwares".
- www.01net.com est classé "jaune" parce qu'en s'inscrivant sur ce site, SiteAdvisor a reçu par la suite en moyenne 6 e-mails par semaine.



L'image ci-dessus peut-être reproduite en recherchant le mot clé "SiteAdvisor" sur Google.fr.

Ce résultat est un peu surprenant parce que ces sites ne sont pas connus comme étant notoirement malfaisants. La notation affectée par SiteAdvisor semble justifiée puisque les critères ayant amené à cette notation sont précisés. Cependant ces critères ne correspondent pas vraiment aux critères de dangerosité intuitifs. En particulier le fait de laisser son adresse e-mail sur un site web entraine généralement toujours une réception de courriers publicitaires. Pourquoi cela est-il jugé dangereux par SiteAdvisor ?

Les produits concurrents

Il existe plusieurs produits similaires à SiteAdvisor. La plupart de ces produits ont été développées par des sociétés indépendantes qui ont été ensuite rachetées par des éditeurs antivirus pour compléter leurs offres. Plusieurs acquisitions de ce type ont eu lieu en 2007.

Voici les produits que nous avons identifiés :

- TrendProtect (Trend Micro) : www.trendsecure.com/portal/en-US/free_security_tools/trendprotect.php
- LinkScanner (Grisoft AVG) : http://linkscanner.com/ et http://linkscanner.explabs.com/
- Finjan SecureBrowsing (Finjan Inc.) : http://securebrowsing.finjan.com

Nous n'avons pas fait d'étude de ces produits. Mais une analyse rapide des articles publiés sur Internet à leurs propos et en particulier les tests publiés par "PC Magazine" (www.pcmag.com) nous ont permis de dégager les éléments de comparaisons suivants :

SiteAdvisor ne teste pas la présence de code agressif ("exploits" susceptibles d'infecter l'internaute lorsqu'il visite le site) dans les pages web visitées, alors que les autres solutions le font. La notation SiteAdvisor tient compte en fait simplement des éléments suivants :

- Le site propose-t-il des fichiers en téléchargement qui peuvent être dangereux ?
- Risque-t-on de recevoir du spam si l'on y laisse son adresse e-mail sur le site ?
- Le site a-t-il bonne réputation ? Est-il lié à des sites ayant bonne réputation ? Utilise-t-il beaucoup de fenêtre pop-up ?

La notation de SiteAdvisor ne se fait pas sur chaque page visitée, mais sur le site global : une note SiteAdvisor est associée à l'ensemble du site web. La note est attribuée au moyen de campagnes de tests faites à l'avance et non au moment ou l'internaute demande à visiter ce site.

Par contre SiteAdvisor donne un résultat plus détaillé et plus facile à comprendre : il explicite clairement la raison pour laquelle la notation est rouge ou verte.

Pour la fonction de recherche des codes hostiles ("exploits") dans les pages visitées, LinkScanner semble souvent jugé comme le plus pertinent.

Conclusion

SiteAdvisor a des côtés séduisants. Il est simple à installer et très intuitif. Cela en fait un bon candidat comme un outil de sensibilisation aux risques induits par la navigation sur Internet. Par contre les résultats produits par l'outil nous ont un peu déçus. En particulier le fait qu'il ne sache pas identifier qu'une page web contienne un code agressif ("exploit" susceptible d'infecter l'internaute lorsqu'il visite le site) nous parait une limitation gênante.

Pour plus d'information

- Description détaillée de SiteAdvisor :
  http://www.siteadvisor.com/download/ff_learnmore.html
  http://www.siteadvisor.com/press/faqs.html

- Comparatif entre SiteAdvisor, TrendProtect et LinkScanner par PC Magazine :
  http://www.pcmag.com/article2/0,2817,2113198,00.asp