Analysis of the "SiteAdvisor" McAfee product

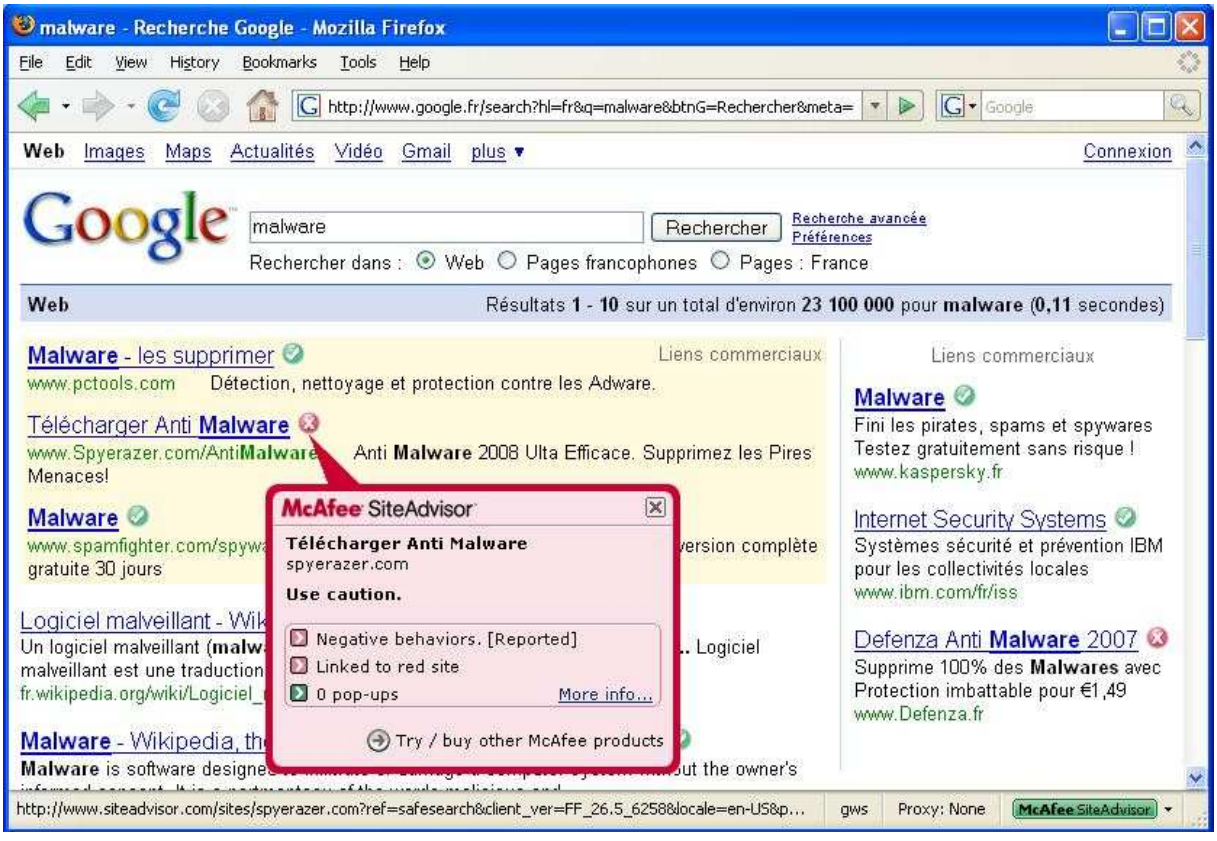
One of our members asked for our opinion about the McAfee "SiteAdvisor" piece of software (www.siteadvisor.com). In this context, we performed an overall analysis on that product, and we present you the results we got.

Introducing SiteAdvisor

SiteAdvisor is a free product that can be plugged into Firefox or Internet Explorer web browsers, and aims at making Internet web browsing safer.

There is also a non-free version of the product, named "SiteAdvisor Plus", which extends the basic features of the free version, which firstly integrates "SiteAdvisor" in e-mails and instant messaging tools (in addition to web browsers) and secondly provides the possibility to deny access to the websites deemed not safe. This non-free version has not been studied.

To achieve that goal, SiteAdvisor complements the results retrieved through the most popular search engines (such as Google, YahooSearch or LiveSearch) by adding in the result page, visual marks indicating if the listed web sites are safe to visit or not (see picture below).



The visual marks are as follow:

- A green mark for a safe site,
- A red mark for a dangerous site,
- A yellow mark for a suspicious site.
- A grey mark for an unrated site (which has not been rated yet by SiteAdvisor).

SiteAdvisor also permanently displays in the bottom right corner of the browser a field that rates the safety of the current visited web site. In the example above, the green button "McAfee SiteAdvisor" indicates that the current web site "www.google.fr" is deemed safe.

Technical analysis of SiteAdvisor

To better understand how SiteAdvisor works and to know the information it sends out to its reference site (the site that host the database and gather ratings for visited websites), we observed the network traffic produced by the SiteAdvisor plug-in. Our test campaign was done using Firefox.

During our tests we observed 3 types of requests generated by SiteAdvisor:

- The "Ping" request checks network connectivity.
- The "Query" request retrieves the rating for a website.
- The "MultiQuery" request retrieves the rating for a set of websites.

We describe in detail these requests below. To sum-up details, we can tell that the observed behaviour is consistent with what we could have imagined. That is a good point.

"Ping" Request:

Example of a "Ping" query we observed during the 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
```

Obviously this request is used to check the version of the SiteAdvisor Plugin. But at the same time it also sends client data to the "SiteAdvisor.com" site: version of Firefox, User identification (UID).

The answer returned by the "siteadvisor.com" web site is less understandable. Here is the answer we got for the above "Ping" query:

```
<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>
```

Clearly this response contains URLs ("location" parameters below) to download data. According to the pathnames used, it should be data to update SiteAdvisor plug-in on Internet Explorer or Firefox. Further analysis of the files "SiteAdv.pak" and "search.dat" (they both contain the Javascript code) could be interesting to better understand how the product works.

"Query" Request:

Example query "Query" we observed during the 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
```

This "Query" request has been generated by SiteAdvisor to query the SiteAdvisor database for the site www.crackz.ws.

Here is the response received for this query:

```
<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>
```

This response is quite readable. It shows that the website is based in Holland (**Location country="NL**"), and that its overall rating will be red (**Classification code="WARN" color="red"**). Then come the details for that rating: Is it possible to download dangerous files on this site? Are personal information at risk? Etc…

"MultiQuery" Request:

The "MultiQuery" request is quite similar to the "Query" request, except that this time the request is about a set of web sites (instead of a single web site).

Here is an example of a "MultiQuery" we observed during our tests:

> 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

We can see here that this "MultiQuery" encompasses ten websites, described by parameters "Name_1" to "Name_10".

The result for each of them is identical to what we presented for the "Query" request above.

Specific concerns

Could McAfee spy my internet activities if I use SiteAdvisor?

One may fear that the information sent by the "SiteAdvisor" plugins to "siteadvisor.com" reveal the habits of the user or transmit sensitive information.

This is true in part. At least, the names of the visited websites (or retrieved through Google) are indeed sent to "SiteAdvisor.com." However the information sent that way is very limited:

- Only the name of the site (for example www.microsoft.com) is sent, rather than the full URL (e.g. www.microsoft.com/technology/mobility/item).
- When parameters are used in URLs (for example an account name or a password), they are not included in the data sent to "SiteAdvisor.com".

From our point of view the information gathered this way remains limited.

Note: It would have been possible to reduce the information sent to SiteAdvisor by just sending the MD5 hash of the visited the site, rather than its name in clear text. If this site is not already known by SiteAdvisor, that latter has then no way to know what site it is, which limits the collected information. It would, however, also have a negative effect since SiteAdvisor could not know the new web sites it should add to its upcoming test campaign (for rating them).

The SiteAdvisor policy about collected data

SiteAdvisor states in its charter that it collects data about the use of SiteAdvisor, but that these data are anonymous (they are not associated with a person), and exists only for people who agreed to participate in the "PIP" (Product Improvement Program).

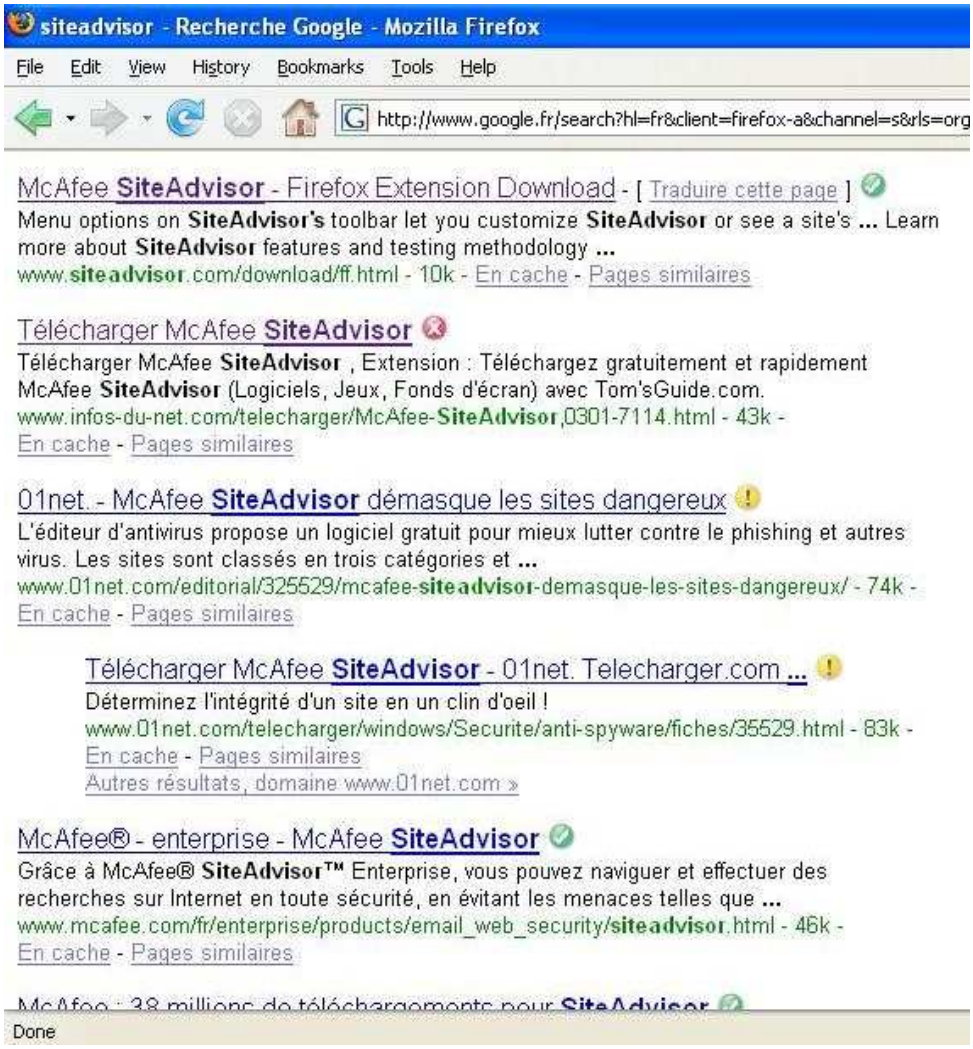
In September 2007, SiteAdvisor announced that it loosens its charter and gives itself the right to transmit the anonymous collected data to "Partners" (cf. announcement http://blog.siteadvisor.com/2007/09/change_to_our_privacy_policy.shtml).

We found that the terms of the charter are quite reasonable. But the change that occurred in September 2007 and the transfer of the collected data to unknown third parties is quite worrying.

Product efficiency

During our tests, we found some SiteAdvisor results quite surprising.
For example, the following French sites are classified as suspects by SiteAdvisor (see picture):

- www.infos-du-net.com is rated as "red" because SiteAdvisor says it had downloaded from the site two programs which were identified to be "malwares".
- www.01net.com is rated as "yellow" because SiteAdvisor says it had received an average of six e-mails per week after leaving its email address on the site. That is considered as SPAM.



The picture below was obtained by searching the keyword "SiteAdvisor" on Google.fr.

This result is somewhat surprising because these sites are not known to be notoriously evil. The rating assigned by SiteAdvisor seems justified because the criteria which led to this rating are clearly explained. However, these criteria are not really the criteria we would have chosen to classify a site as dangerous. In particular, when you leave your e-mail on a website, it is quite likely that you will later receive e-mail from that site. Why is it considered as dangerous by SiteAdvisor?

Competitor products

There are several products similar to SiteAdvisor. Most of these products were developed by independent companies which were subsequently purchased by antivirus companies to enhance their offers. Most of such acquisitions took place in 2007.

Below is list of competitor products we identified:

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

We did not study these products. But a quick analysis of articles published about them and in particular the tests published by "PC Magazine" (www.pcmag.com) led us to the following findings:

SiteAdvisor does not test for the presence of hostile code ("exploits" that could infect the user when he visits the site) in the web pages visited. The other products do these tests. In fact, the SiteAdvisor ratings just take into account the following elements:

- Does the site propose downloadable files which are dangerous (malwares)?
- Will you receive spams if you leave your e-mail address on the site?
- Does a site have a good reputation? Do their affiliated web sites have a good reputation too? Does the site use excessive pop-ups?

SiteAdvisor does not rate each visited pages. The rating applies to the whole site and is established by running a set of tests against the site. Test campaigns are performed in advance by SiteAdvisor (not at the time the user visits the site).

SiteAdvisor reports are more detailed and easier to understand than the ones produced by the other products. SiteAdvisor reports clearly explain why the rating is red or green.

In the field of testing visited pages for hostile code (exploits), LinkScanner is often known to be the most relevant product.

Conclusion

From most of its aspects SiteAdvisor is quite appealing. It is simple to install and very intuitive. This makes it a good candidate as a tool to raise awareness on the risks associated with Internet browsing. But we were a bit disappointed by the ratings produced by the tool for some sites. Furthermore, the fact that SiteAdvisor is not able to identify hostile content ("exploit" that could infect the user when visiting the site) embedded in visited web pages is for us a severe limitation.

For more information

- Detailed description of SiteAdvisor:
  http://www.siteadvisor.com/download/ff_learnmore.html
  http://www.siteadvisor.com/press/faqs.html

- Comparison between SiteAdvisor, TrendProtect and LinkScanner by PC Magazine:
  http://www.pcmag.com/article2/0,2817,2113198,00.asp