

## RE: Anti-spyware Beta from Microsoft available

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2005-01/0068.html>

---

*From:* Shaffer, Bruce (*BShaffer\_at\_PRAC.com*)

*Date:* 01/13/05

To: 'Eric McCarty' <eric@piteduncan.com>, "Shaffer, Bruce" <BShaffer@PRAC.com>, 'Focus-MS' <focus@piteduncan.com>  
Date: Thu, 13 Jan 2005 07:37:34 -0500

Running the default scan in Spybot and Adaware runs in the context of the current user and does not check Documents and Settings\... for other users. Running the full scan, at least in Adaware, does not check current running processes as it does in the user scan, but does check everything from the root down provided you have selected c:\ as the starting point.

I wouldn't put a whole lot on the software continuing to run after the license expires. MS is controlling who can get updates, any and all updates including service packs, based on the validity of the installation key. They have a rather large database of publicly known cd keys as well as knowing exactly which keys they've already generated in order to defeat the key generators that can be found on the net. When the license expires, chances are extremely good that you will not be able to update it until you've renewed your subscription.

As far as the other two not being current: no signature based algorithm is current by definition. MS is planning on issuing monthly updates along with the security bulletin. At least with Adaware and Spybot you can update just before you run and they have been known to issue new updates on contiguous days, not necessarily contiguous months as MS is considering. They did state that they plan to have interim signatures available for more immediate threats that they consider to be a major threat.

MS does fairly well in the OS and Office categories, (security concerns aside), and there past history in delving into areas such as antivirus (anyone remember that less than useless program MSAV?), firewall, backups, IDS, etc. with somewhat less than stellar results.

I use the Norton A/V Corporate edition and quite frankly, it has an adverse effect on my ability to relax but, it gives me something to do with my free time. I don't intend to turn this into a blue bashing or a Symantec bashing so, enough said about those two.

-B-

-----Original Message-----

From: Eric McCarty [mailto:eric@piteduncan.com]

RE: Anti-spyware Beta from Microsoft available

SecurityFocus Microsoft: RE: Anti-spyware Beta from Microsoft available

Sent: Monday, January 10, 2005 4:29 PM  
To: Shaffer, Bruce; Focus-MS  
Subject: RE: Anti-spyware Beta from Microsoft available

Expired Software <> Unlicensed software

I believe that the software will cease to function as opposed to violating any sort of licensing agreements.

I believe that running the Intelligent scan is far different from running the full scan, which may be why there are different results with different spyware products. So far I have had great luck with Microsoft's Anti-spyware, but have found that spybot and adaware neither find even 90% of the spyware and are often useless against the newest spyware.

We pay an arm and a leg for products like Norton A/V Corporate Edition, I venture to guess we would do the Same with Microsoft Anti-Spam Corporate Edition.

Eric

-----Original Message-----

From: Shaffer, Bruce [mailto:BSshaffer@PRAC.com]  
Sent: Monday, January 10, 2005 12:50 PM  
To: 'Focus-MS'  
Subject: RE: Anti-spyware Beta from Microsoft available

I just installed the MS Antispyware tool with the default install, updated the signatures then ran the default scan. It came back with no spyware detected.

I then brought up Spybot, updated his files and ran the default scan. He returned 5 registry keys, a pile of cookies and a browser hijack. Cleaned this up.

Next I ran Adaware, updated files, etc. Adaware came back with 10 more cookies.

The point I am trying to make here is that there is so much spyware out there and antispyware is so young and doesn't enjoy the information sharing between researchers that AV does, nothing will catch even 50% of known spyware.

I read a review in the last couple of months that stated that there were approximately 29.5 million pieces of known spyware and of those, 5 million were programs. The number may be a little high, but if you think about it, there are about 100,000 known viruses and worms authored in the past 19 years and none of these were commissioned by marketers. People get paid to write spyware so the 8 figure total is not unrealistic.

RE: Anti-spyware Beta from Microsoft available

SecurityFocus Microsoft: RE: Anti-spyware Beta from Microsoft available

If we had a program that could incorporate all of these signatures, would we be able to do daily or weekly scans? How about monthly?

One thing I haven't seen anyone comment on yet is: does this drop its own spyware? Most of the \$\$ products do, Ad-aware and Spybot do not.

For home machines I overlap my favorite two products, for enterprise, I use Spybot only. I would be leery of installing any "free for a time" software on the enterprise. What's going to happen when you don't get budget to purchase this next July? More \$\$ for the MS lawyers or a scramble for your techs to uninstall before someone notices you're using unlicensed software?

Just my opinion.

D. Bruce Shaffer, CISSP  
Information Security Engineer  
PRAC.COM

-----Original Message-----

From: Yuen, Steven [mailto:Steven.Yuen@ubs.com]  
Sent: Monday, January 10, 2005 11:59 AM  
To: 'John Fleming'; 'Rod Serbanescu'; 'Glenn S.'; 'Danny'; 'Focus-MS'  
Subject: RE: Anti-spyware Beta from Microsoft available

I have been using it as well and it is more thorough than some of the others I've used. So far, it is stable.

-----Original Message-----

From: John Fleming [mailto:jfleming@creativeventuresofboca.com]  
Sent: Friday, January 07, 2005 4:39 PM  
To: 'Rod Serbanescu'; 'Glenn S.'; 'Danny'; 'Focus-MS'  
Subject: RE: Anti-spyware Beta from Microsoft available

I only installed it on one machine so far and have had no problems. Seems to work very well. A little slow it seems when removing spy ware, but I believe it may be more thorough plus it is a Beta version. I'm sure there will be many improvements. An MSI package would be nice to rollout using Group Policy.

-----Original Message-----

From: Rod Serbanescu [mailto:rods@loanstillpayday.com]  
Sent: Friday, January 07, 2005 3:00 PM  
To: 'Glenn S.'; 'Danny'; 'Focus-MS'  
Subject: RE: Anti-spyware Beta from Microsoft available

I've already installed it on 4 machines and it works great, it beats all

RE: Anti-spyware Beta from Microsoft available

SecurityFocus Microsoft: RE: Anti-spyware Beta from Microsoft available

the other ones that are out there put together. The only problem with it atm is that it is still beta and sometimes it freezes for a bit, other then that it works great and has options that many other apps are lacking. This is a welcome change.

-----Original Message-----

From: Glenn S. [mailto:glenn@secureinformation.net]  
Sent: Thursday, January 06, 2005 3:27 PM  
To: Danny; Focus-MS  
Subject: Re: Anti-spyware Beta from Microsoft available

Microsoft recently acquired Anti-spyware company Giant and is now making their Anti-spyware tool available for free download if anyone is interested:

<http://www.microsoft.com/athome/security/spyware/software/default.aspx>

----- Original Message -----

From: "Danny" <nocmonkey@gmail.com>  
To: "Focus-MS" <focus-ms@securityfocus.com>  
Sent: Thursday, January 06, 2005 9:38 AM  
Subject: Anti-spyware Beta from Microsoft available

>  
> <http://www.microsoft.com/downloads/details.aspx?FamilyID=321cd7a2-6a57-4c57-a8bd-dbf62eda9671&DisplayLang=en>

>  
>

-----  
---

>

-----  
---

>

-----  
---

-----  
---

-----  
---

-----  
---

-----  
---

Please do not transmit orders or instructions regarding a UBS account by email. The information provided in this email or any attachments is not an official transaction confirmation or account statement. For your

RE: Anti-spyware Beta from Microsoft available

SecurityFocus Microsoft: RE: Anti-spyware Beta from Microsoft available

protection,  
do not include account numbers, Social Security numbers, credit card  
numbers, passwords or other non-public information in your email.  
Because  
the information contained in this message may be privileged,  
confidential,  
proprietary or otherwise protected from disclosure, please notify us  
immediately by replying to this message and deleting it from your  
computer  
if you have received this communication in error. Thank you.  
UBS Financial Services Inc.  
UBS International Inc.

-----  
---  
-----  
---  
-----  
---  
-----  
---  
-----  
-----  
-----  
-----  
-----