

Forum:[Hack Forums](#)

Thread: [\[FREE\] Malwarebytes BETA Anti-Exploit - Protect yourself from Java DRIVE BYs](#)

Lightning_ - October 27, 2013, 3:25 am

Hi guys,

Not sure if this has been posted before, but as we all know, no Windows AV kit is complete without Malwarebytes.

Turns out they have a beta of one of their up-and-coming releases, an anti exploit kit. Info cut directly from their site:

Quote:Malwarebytes Anti-Exploit BETA protects you from zero-day exploits targeting browser and application vulnerabilities. Its proprietary technology protects you in that critical period between the release of a new exploit and its subsequent security patch. And, unlike antivirus products, Malwarebytes Anti-Exploit BETA proactively prevents the exploit from installing its payload. Before it can do damage.

I recommend everyone check out the page for this product, as it's safely defended me against two Java drive-by installations that I purposely visited for the purpose of testing it out (I'll provide screenshots later when I'm on a faster PC)

[The page for it can be found by clicking here.](#)

Hope this saves people from some trouble, and I'm sorry for any pro-RATers on HF whose plans this destroys ?

phybe? - October 27, 2013, 10:38 am

Interesting, did not know they came out with this.

I absolutely love how they are always expanding their product line. Thanks for the share!

T e s s e r a c t - October 27, 2013, 11:35 am

I couldn't agree more with Phyber. I hope they do not charge users for a full version later on. This seems like an awesome fine and reliable software, I love malwarebytes.

adampelletgun - October 27, 2013, 11:37 am

Thanks for the news.

Downloading now.

Gr0nica - October 27, 2013, 2:32 pm

Nice never knew about that thanks for sharing ?

yesLAD - October 27, 2013, 2:54 pm

Probably wouldn't of noticed if you hadn't made a thread, thanks.

Lightning_ - October 27, 2013, 6:37 pm

You guys are all welcome :)

I was browsing a suspicious site earlier, the site tried to lock up my browser - it looked like the AFP Ransomware.. idk what that's called outside of Australia, but it shows the Australian Federal Police logo and wants you to pay \$30 or something to some Russian account or you'll get arrested.

Out of the blue I got some message from AE before quickly being redirected to malwarebytes.org? and then Malwarebytes stepped up and said that a suspicious connection had been blocked - no suspicious files were detected though, so it clearly does something haha :P

madTRiiKs - October 27, 2013, 6:39 pm

Just downloaded it, thanks for the share. Never knew they had this

???LL - October 27, 2013, 6:44 pm

Can I use Malware bytes anti malware and anti exploit together?

?Ñâzg?! - October 27, 2013, 6:46 pm

I tried it and it blocked MOST exploits that I used against it so far

java applet attack (exploit detected)

adobe_flash_mp4_cppt (exploit success mbam did not detect exploit)

Internet Explorer CSS SetUserClip Memory Corruption (Exploit detected AFTER memory corruption. the computer slowed down dramaticly)

not sure how this works exactly.

The only reason why adobe flash player got through is because mbam does not yet support adobe flash player

ok so I think the way it works is by simply detecting the executable payload being sent when a exploit is used

im not sure how effective this is and if issues may occur

it cant stop buffer overflows and memory corruption leaks from uccoring but it does stop a excutable payload

Exact - October 27, 2013, 6:49 pm

I thought that MBAM pro blocked 0day exploits though? Why would they release a free program that does this, and lose potential pro buyers?

Quote:Malicious Website Protection Blocks Access to Known and Zero Day Malicious Web Content

EDIT:

[img]http://img62.imageshack.us/img62/3217/qfk9.png[/img]

Doesn't even work for me. I think it might be that I have MBAM pro already (even though it says it's compatible) or that I'm on Windows 8.1. It only says Windows 8 is compatible, not 8.1 but I thought it would work.

Lightning_ - October 27, 2013, 6:59 pm

According to their page it's proactive - but how it's proactive I'm not sure. I'd really like to know how it works too, because it's pretty damn good at it's job, and I'm confused as to why no-one else has

assumed a similar approach in the past? I thought Symantec were up there thanks to all that money they have.. but apparently not. ?

(Oct 27, 2013 06:44 PM)???LL Wrote: [\[CITE\]](#) Can I use Malware bytes anti malware and anti exploit together? You can my friend, it's designed to be used this way.?

(Oct 27, 2013 06:49 PM)Exact Wrote: [\[CITE\]](#) I thought that MBAM pro blocked 0day exploits though? Why would they release a free program that does this, and lose potential pro buyers? This is a Beta of a new program that's kind of like a feature when compared to MBAM - I'm assuming they're going to implement it later on. And it does, but it's definitely not this efficient - AE seems to take a different approach.

(Oct 27, 2013 06:49 PM)Exact Wrote: [\[CITE\]](#) Spoiler [\(Click to View\)](#)
[img]http://img62.imageshack.us/img62/3217/qfk9.png[/img]

Doesn't even work for me. I think it might be that I have MBAM pro already (even though it says it's compatible) or that I'm on Windows 8.1. It only says Windows 8 is compatible, not 8.1 but I thought it would work. I have MBAM pro and I'm running Windows 8.1 - it's probably something else. I got a very similar error when installing MBAM on one of my clients' systems that had DC on it, so maybe you should try running it in safemode or something?

It is only a BETA release after all.

Exact - October 28, 2013, 12:25 pm

(Oct 27, 2013 06:59 PM)Lightning_ Wrote: [\[CITE\]](#) According to their page it's proactive - but how it's proactive I'm not sure. I'd really like to know how it works too, because it's pretty damn good at it's job, and I'm confused as to why no-one else has assumed a similar approach in the past? I thought Symantec were up there thanks to all that money they have.. but apparently not. ?

You can my friend, it's designed to be used this way.?

This is a Beta of a new program that's kind of like a feature when compared to MBAM - I'm assuming they're going to implement it later on. And it does, but it's definitely not this efficient - AE seems to take a different approach.

I have MBAM pro and I'm running Windows 8.1 - it's probably something else. I got a very similar error when installing MBAM on one of my clients' systems that had DC on it, so maybe you should try running it in safemode or something?

It is only a BETA release after all.

Malwarebytes was installed before I upgraded to 8.1. I will give it a while before trying MBAM AE installation again.

Lightning_ - November 2, 2013, 2:57 am

(Oct 28, 2013 12:25 PM)Exact Wrote: [\[CITE\]](#) I will give it a while before trying MBAM AE installation again. That could work too :P If it's not already integrated by then, that is.

Waist - November 2, 2013, 3:23 pm

Downloading as we speak, thanks op.

enjoy your new rep.

?Detox - November 3, 2013, 4:48 am

Malwarebytes definitely comes in handy, and I love the tool, also the website blocking.

Although it sometimes tend to block sites that are completely fine, which is kinda annoying. Nonetheless, you can just add exceptions right-clicking the MB icon in system tray and by clicking "Add to ignore list", then finding the corresponding IP for that website.

bb1ox1bb - November 3, 2013, 11:50 am

(Oct 27, 2013 06:49 PM)Exact Wrote: [\[CITE\]](#) I thought that MBAM pro blocked Oday exploits though? Why would they release a free program that does this, and lose potential pro buyers?

EDIT:

[img]http://img62.imageshack.us/img62/3217/qfk9.png[/img]

Doesn't even work for me. I think it might be that I have MBAM pro already (even though it says it's compatible) or that I'm on Windows 8.1. It only says Windows 8 is compatible, not 8.1 but I thought it would work.

probably you are installing sandboxed

Lightning_ - November 6, 2013, 9:02 am

(Nov 3, 2013 05:48 AM)?Detox Wrote: [\[CITE\]](#) Nonetheless, you can just add exceptions right-clicking the MB icon in system tray and by clicking "Add to ignore list", then finding the corresponding IP for that website. I wasn't aware you could do this! Thank you haha. Saves me a lot of time when browsing Anime sites, as they all seem to be flagged.

I'm an avid Baka member with an FTV subscription of course, I just sometimes can't be bothered waiting for new episode releases. ?

hutt132 - November 8, 2013, 11:41 pm

Thanks for sharing this. Going to install it soon.

Lightning_ - November 9, 2013, 3:40 am

(Nov 9, 2013 12:41 AM)hutt132 Wrote: [\[CITE\]](#) Thanks for sharing this. Going to install it soon. You're welcome bro :) Hope it saves you some trouble like it has me :)

Huskar - November 9, 2013, 11:04 am

I love malwarebytes their the best :)

Thanks for posting this !

SilverHick - November 11, 2013, 4:03 am

I was using it but it blocks netflix silverlight so I turned it off.

Lightning_ - November 11, 2013, 4:12 am

(Nov 11, 2013 05:03 AM)Duhuh Wrote: [\[CITE\]](#) I was using it but it blocks netflix silverlight so I turned it off. Does it really?

I use an opensource alternative to silverlight, and I don't use netflix on Windows PCs, so I wouldn't know.

Shouldn't much matter in the future, silverlight is predominantly known for it's susceptibility to exploitation.

[Bye-bye Silverlight says Netflix, hello modern standards.](#)

koolfrank - November 14, 2013, 5:38 pm

thanks for this share!! downloading it now!!

Lightning_ - November 14, 2013, 6:30 pm

(Nov 14, 2013 06:38 PM)koolfrank Wrote: [\[CITE\]](#) thanks for this share!! downloading it now!!You're completely welcome :)

The page was down for about 12 hours with the message 'Implementation in progress...'
Not sure what that meant, but it's back up now.

Maximum - November 15, 2013, 1:56 pm

Trying this beta out and installing this now, thanks for the share!