



# Malwarebytes ANTI-EXPLOIT

## Live Exploit test results

Here at Malwarebytes, we do our best to innovate the realm of online threat protection for our users and honestly, everyone who uses a computer. To that end, we have developed Malwarebytes Anti-Exploit as the next generation in exploit blocking technology.

Malwarebytes Anti-Exploit was designed to block exploits from dropping malicious software onto a victim system, which is one of the most common infection methods seen today. During the course of its operations, Malwarebytes Anti-Exploit adds an additional shield to a user's pre-existing security solution.

Think of Anti-Malware technology as created to provide a user with a bulletproof vest to deal with oncoming fire, Malwarebytes Anti-Exploit catches the bullet before it ever gets a chance to hit.

In order to prove Malwarebytes Anti-Exploit has the ability to block exploit drops, we went ahead and put it to the test against the most common and dangerous exploit kits currently found in the wild.



In order to make sure our tests were legitimate, we reached out to the best authority on the threat of exploit kits; world-renowned threat researcher, Kafeine. He performed an in-depth performance measure of Malwarebytes Anti-Exploit against the various exploits; we have reprinted the following results with Kafeine's permission:

### Defeated:



### Protected:





## Detailed Results from Tests\*

| Exploit Kit            | Exploit CVE        | Target Application | App Ver    | Result          |
|------------------------|--------------------|--------------------|------------|-----------------|
| <b>Nuclear Pack</b>    |                    |                    |            | <b>Passed</b>   |
|                        | CVE-2013-2551      | Internet Explorer  | 8.0        | Exploit Blocked |
|                        | CVE-2013-2423      | Java               | 7.0.0.07   | Exploit Blocked |
|                        | CVE-2010-0188      | Adobe Reader       | 9.3.0.148  | Exploit Blocked |
|                        | CVE-2013-2460      | Java               | 7.0.21     | Exploit Blocked |
|                        | CVE-2014-0322      | Internet Explorer  | 10.0       | Exploit Blocked |
| <b>Angler EK</b>       |                    |                    |            | <b>Passed</b>   |
|                        | CVE-2013-2551      | Internet Explorer  | 8.0        | Exploit Blocked |
|                        | CVE-2014-0322      | Internet Explorer  | 10.0       | Exploit Blocked |
|                        | CVE-2014-0497      | Adobe Flash Player | 5.1.20513  | Exploit Blocked |
| <b>Infinity EK</b>     |                    |                    |            | <b>Passed</b>   |
|                        | CVE-2013-2551      | Internet Explorer  | 8.0        | Exploit Blocked |
|                        | CVE-2014-0322      | Internet Explorer  | 10.0       | Exploit Blocked |
|                        | CVE-2013-3896      | Silverlight        | 5.1.20513  | Exploit Blocked |
| <b>FlashPack EK</b>    |                    |                    |            | <b>Passed</b>   |
|                        | CVE-2013-2551      | Internet Explorer  | 8.0        | Exploit Blocked |
|                        | CVE-2013-2465/2471 | Java               | 7.0.21     | Exploit Blocked |
|                        | CVE-2014-0497      | Adobe Flash Player | 13.0.0.182 | Exploit Blocked |
|                        | CVE-2014-0515      | Adobe Flash Player | 13.0.0.182 | Exploit Blocked |
| <b>Magnitude EK</b>    |                    |                    |            | <b>Passed</b>   |
|                        | CVE-2013-2551      | Internet Explorer  | 8.0        | Exploit Blocked |
|                        | CVE-2013-2471      | Java               | 6.u.45     | Exploit Blocked |
| <b>Fiesta EK</b>       |                    |                    |            | <b>Passed</b>   |
|                        | CVE-2013-2551      | Internet Explorer  | 8.0        | Exploit Blocked |
|                        | CVE-2014-0497      | Adobe Flash Player | 12.0.0.38  | Exploit Blocked |
| <b>Grandsoft EK</b>    |                    |                    |            | <b>Passed</b>   |
|                        | CVE-2013-5329      | Adobe Flash Player | 12.0.0.38  | Exploit Blocked |
|                        | CVE-2013-2463      | Java               | 6.u.45     | Exploit Blocked |
| <b>Sweet Orange EK</b> |                    |                    |            | <b>Passed</b>   |
|                        | CVE-2013-2460      | Java               | 7.0.21     | Exploit Blocked |
|                        | CVE-2014-0497      | Adobe Flash Player | 12.0.0.38  | Exploit Blocked |
| <b>Styx EK</b>         |                    |                    |            | <b>Passed</b>   |
|                        | CVE-2013-2551      | Internet Explorer  | 8.0        | Exploit Blocked |
|                        | CVE-2013-0634      | Adobe Flash Player | 11.5.502   | Exploit Blocked |
|                        | CVE-2013-3896      | Silverlight        | 5.1.20513  | Exploit Blocked |
| <b>RIG</b>             |                    |                    |            | <b>Passed</b>   |
|                        | CVE-2013-0634      | Adobe Flash Player | 11.5.502   | Exploit Blocked |
|                        | CVE-2014-0322      | Internet Explorer  | 10         | Exploit Blocked |
|                        | CVE-2014-0497      | Adobe Flash Player | 12.0.0.44  | Exploit Blocked |
|                        | CVE-2013-0074/3896 | Silverlight        | 5.1.10411  | Exploit Blocked |
| <b>Gondad</b>          |                    |                    |            | <b>Passed</b>   |
|                        | CVE-2013-0634      | Adobe Flash Player | 11.5.502   | Exploit Blocked |

\*Note: Exploits that either crashed the browser or failed to drop any malicious payload were not included in these results

\*\*Full test details can be found at <http://malware.dontneedcoffee.com/2014/06/mbae.html>