

[TOOL] Apache mod_evasive – Evasive Maneuvers for Apache

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00018.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 7 Feb 2007 17:58:06 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Apache mod_evasive – Evasive Maneuvers for Apache

SUMMARY

DETAILS

mod_evasive is an evasive maneuvers module for Apache to provide evasive action in the event of an HTTP DoS or DDoS attack or brute force attack. It is also designed to be a detection and network management tool, and can be easily configured to talk to ipchains, firewalls, routers, and etcetera. mod_evasive presently reports abuses via email and syslog facilities.

Detection is performed by creating an internal dynamic hash table of IP Addresses and URIs, and denying any single IP address from any of the following:

- * Requesting the same page more than a few times per second
- * Making more than 50 concurrent requests on the same child per second
- * Making any requests while temporarily blacklisted (on a blocking list)

This method has worked well in both single-server script attacks as well

[TOOL] Apache mod_evasive – Evasive Maneuvers for Apache

as distributed attacks, but just like other evasive tools, is only as useful to the point of bandwidth and processor consumption (e.g. the amount of bandwidth and processor required to receive/process/respond to invalid requests), which is why it's a good idea to integrate this with your firewalls and routers for maximum protection.

This module instantiates for each listener individually, and therefore has a built-in cleanup mechanism and scaling capabilities. Because of this per-child design, legitimate requests are never compromised (even from proxies and NAT addresses) but only scripted attacks. Even a user repeatedly clicking on 'reload' should not be affected unless they do it maliciously. mod_evasive is fully tweakable through the Apache configuration file, easy to incorporate into your web server, and easy to use.

ADDITIONAL INFORMATION

The information has been provided by Jonathan A. Zdziarski.
To keep updated with the tool visit the project's homepage at:
<http://www.zdziarski.com/projects/mod_evasive/>
http://www.zdziarski.com/projects/mod_evasive/

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.