

Re: DDOS problem from Bangkok, Thailand

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2008-03/msg00008.html>

- *From:* "Adrian Penisoara" <ady@xxxxxxxxxxxxxxxx>
 - *Date:* Thu, 6 Mar 2008 18:00:14 +0200
-

Hi,

On Thu, Mar 6, 2008 at 3:04 PM, Volker <volker@xxxxxxxxxxx> wrote:

On 03/06/08 11:58, kamolpat@xxxxxxxxxxxxxxxx wrote:

Dear Security team,

I'm Kamolpat Pornatiwiwat, Sys admin of DMaccess Co., Ltd. I'm got the problem, My FreeBSD 6.0 got Dos attacked. What should I do? At the present, I decide to stop apache and leave only mail feature on functioning. Any guide/recommend/solution will be appreciated.

More detail about my server:

=====

FreeBSD 6.0 apache-1.3.34_4 php5-5.1.2_1 MySQL 5.0.20

php.ini

=====

.....
.....
; Resource Limits ;
.....

max_execution_time = 30 ; Maximum execution time of each script, in seconds
max_input_time = 60 ; Maximum amount of time each script may spend parsing r
memory_limit = 32M (at the beginning it is 8M, I change to 32MB since the cause of httpd-error.log, however, it still the error as the following showed on httpd-error.log

FILE:/var/log/httpd-error.log

=====

Allowed memory size of 33554432 bytes exhausted happend like this all over the log

Re: DDOS problem from Bangkok, Thailand

Thanks in Advanced,
Kamolpat Pornatiwiwat, Sys admin DMaccess Co., Ltd.

Kamolpat,

without being a member of the secteam, I like to jump in here.

\${subject} contains "DDoS" but I don't see any signs of a DDoS from what you're describing. Sure it might be a DoS attack but that needs carefully inspection of your log file (look for specially crafted URLs being requested).

To me, exhausted memory situations are more likely looking like application problems (read as: bad code). With just that exhausted memory message given, it's guesswork to tell more but you may want to check PHP's bug database.

Hmm, I'm wandering -- if you see a simple SYN flood attack (just opening connections without sending an HTTP request) then you should try enabling the `accf_http(9)` mechanism in kernel and using the "AcceptFilter http" Apache configuration.

My 5 cents,
Adrian Penisoara
ROFUG / EnterpriseBSD

freebsd-security@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@xxxxxxxxxxx"