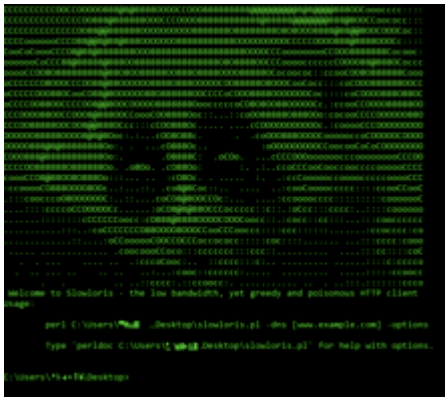
WIKIPEDIA

Slowloris (computer security)

Slowloris is a type of denial of service attack tool invented 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.[1]

Slowloris



Slowloris running on Command Prompt

Original author(s)	RSnake
Initial release	17 June 2009
Stable release	0.7
Written in	Perl
Platform	Cross-platform
Size	36 kb
Type	Hacking tool
Website	ha.ckers.org/slowloris/ (https://web.archive.org/web/20090822001255/http://ha.ckers.org/slowloris/)

Contents

Affected web servers

This includes but is not necessarily limited to the following, per the attack's author:[1]

- Apache 1.x and 2.x
- dhttpd
- Websense "block pages" (unconfirmed)
- Trapeze Wireless Web Portal (unconfirmed)
- Verizon's MI424-WR FIOS Cable modem (unconfirmed)
- Verizon's Motorola Set-top box (port 8082 and requires auth - unconfirmed)
- BeeWare WAF (unconfirmed)
- Deny All WAF (patched) [2]
- Flask

Because Slowloris exploits problems handling thousands of connections, the attack has less of an effect on servers

that handle large numbers of connections well. Proxying servers and caching accelerators such as Varnish, nginx, and Squid have been recommended[3] to mitigate this particular kind of attack. In addition, certain servers are more resilient to the attack by way of their design, including Hiawatha,[4] IIS, lighttpd, Cherokee, and Cisco CSS (http://www.awesometechhome.com/css_csm/css_csm.htm).

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 server 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.[1][5] Since Apache 2.2.15, Apache ships the module mod_reqtimeout as the official solution supported by the developers.[6]

Other mitigating techniques involve setting up reverse proxies, firewalls, load balancers or content switches.[7] 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.[1]

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 flooding DDoS attacks would affect internet access for the government and protesters equally, due to the significant bandwidth they can consume. 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 .[10]

A variant of this attack was used by spam network River City Media to force Gmail servers to send thousands of messages en-bulk, by opening thousands of connections to the Gmail API with message sending requests, then completing them all at once.[11]

Similar software

Since its release, a number of programs have appeared that mimic the function of Slowloris while providing additional functionality, or running in different environments:[12]

- PyLoris – A protocol-agnostic Python implementation supporting Tor and SOCKS proxies.[13]
- Slowloris – A Python 3 implementation of Slowloris with SOCKS proxy support.[14]
- Goloris – Slowloris for nginx, written in Go.[15]
- QSlowloris – An executable form of Slowloris designed to run on Windows, featuring a Qt front end.[16]
- An unnamed PHP version which can be run from a HTTP server.[17]

- SlowHTTPTest – A highly configurable slow attacks simulator, written in C++.[18][19]
- SlowlorisChecker – A Slowloris and Slow POST POC (Proof of concept). Written in Ruby.[20]
- Cyphon - Slowloris for Mac OS X, written in Objective-C.[21]
- sloww - Slowloris implementation written in Node.js.[22]
- dotloris - Slowloris written in .NET Core [23]

See also

- SlowDroid
- Trinoo
- Stacheldraht
- Denial of service
- LAND
- Low Orbit Ion Cannon
- High Orbit Ion Cannon
- ReDoS
- R-U-Dead-Yet

References

1. "Slowloris HTTP DoS" (https://web.archive.org/web/20150426090206/http://ha.ckers.org/slowloris). Archived from the original on 26 April 2015. Retrieved 26 June 2009.
2. "Archived copy" (https://web.archive.org/web/20140201201359/http://www.denyall.com/files/090703-Flash-Presse-contre-Slowloris.pdf) (PDF). Archived from the original (http://www.denyall.com/files/090703-Flash-Presse-contre-Slowloris.pdf) (PDF) on 1 February 2014. Retrieved 15 May 2013.
3. "How to best defend against a "slowloris" DOS attack against an Apache web server?" (http://serverfault.com/a/32472/129773). *serverfault.com*. Retrieved 2016-12-28.
4. "Performance testing while under attack" (https://www.hiawatha-webserver.org/weblog/64). hiawatha-webserver.org. 28 February 2014.
5. "mod_noloris: defending against DoS" (http://bahumbug.wordpress.com/2009/07/01/mod_noloris-defending-against-dos/). niq's soapbox. Retrieved 7 January 2012.
6. "mod_reqtimeout - Apache HTTP Server" (https://httpd.apache.org/docs/2.4/mod/mod_reqtimeout.html). Httpd.apache.org. Retrieved 2013-07-03.
7. Breedijk, Frank (22 June 2009). "Slowloris and Nkiller2 vs. the Cisco CSS load balancer" (http://www.cupfighter.net/index.php/2009/06/slowloris-css/). Cupfighter.net. Retrieved 7 January 2012.
8. Zdrnja, Bojan (23 June 2009). "ISC Diary | Slowloris and Iranian DDoS attacks" (http://isc.sans.org/diary.html?storyid=6622). Isc.sans.org. Retrieved 7 January 2012.
9. [1] (http://iran.whyweprotest.net/general-discussion/2156-list-anti-protester-sites-2.html) Archived (https://web.archive.org/web/20090629152805/http://iran.whyweprotest.net/general-discussion/2156-list-anti-protester-sites-2.html) 29 June 2009 at the Wayback Machine
10. [2] (http://iran.whyweprotest.net/help-iran-online/6194-condensed-list-sites-w-pictures-part-1-a.html) Archived (https://web.archive.org/web/20090811013813/http://iran.whyweprotest.net/help-iran-online/6194-condensed-list-sites-w-pictures-part-1-a.html) 11 August 2009 at the Wayback Machine

11. Vickery, Chris (2017-03-06). "Spammergate: The Fall of an Empire" (https://web.archive.org/web/20170306152831/https://mackeeper.com/blog/post/339-spammergate-the-fall-of-an-empire). *MacKeeper Security Watch*. Archived from the original (https://mackeeper.com/blog/post/339-spammergate-the-fall-of-an-empire) on 2017-03-06.
12. Robert “RSnake” Hansen. "Slowloris" (http://samsclass.info/seminars/slowloris.pdf) (PDF). SecTheory. Retrieved 7 January 2012.
13. "PyLoris" (https://web.archive.org/web/20090715100428/http://motomastyle.com/pyloris/). MotomaSTYLE. 19 June 2009. Archived from the original (http://motomastyle.com/pyloris/) on 15 July 2009. Retrieved 7 January 2012.
14. "Slowloris rewrite in Python" (https://github.com/gkbrk/slowloris). Retrieved 10 May 2017.
15. valyala. "Slowloris for nginx DoS" (https://github.com/valyala/goloris). Retrieved 4 February 2014.
16. "How to help take down gerdab.ir in 5 easy steps" (http://cyberwar4iran.blogspot.com/). cyberwar4iran. 28 June 2009. Retrieved 7 January 2012.
17. "Full Disclosure: apache and squid dos" (http://seclists.org/fulldisclosure/2009/Jun/0207.html). Seclists.org. 19 June 2009. Retrieved 7 January 2012.
18. "Testing Web Servers for Slow HTTP Attacks" (https://community.qualys.com/blogs/securitylabs/2011/09/19/testing-web-servers-for-slow-http-attacks). qualys.com. 19 September 2011. Retrieved 13 January 2012.
19. "shekyan/slowhttptest: Application Layer DoS attack simulator" (https://github.com/shekyan/slowhttptest/). GitHub. Retrieved 2017-04-19.
20. "Simple script to check if some server could be affected by Slowloris attack" (https://github.com/felmoltor/SlowlorisChecker). github.com/felmoltor. 31 December 2012. Retrieved 31 December 2012.
21. abilash. "Slowloris for OSX" (https://github.com/abila5h/Cyphon-DoS). Retrieved 8 April 2017.
22. Davis, Ethan (2018-02-17), *sloww: Lightweight Slowloris attack CLI in Node* (https://github.com/ethanent/sloww), retrieved 2018-02-18
23. Bassel Shmali. "Slowloris written in .Net core" (https://github.com/bass3l/dotloris).

External links

- Slowloris HTTP DoS (https://web.archive.org/web/20090822001255/http://ha.ckers.org/slowloris/)
- hackaday on Slowloris (http://hackaday.com/2009/06/17/slowloris-http-denial-of-service/)
- Apache attacked by a "slow loris" (https://lwn.net/Articles/338407/) article on LWN.net
- Slowloris – a short video (including a demo) (http://www.radware.com//Multimedia/Security_Zone/slowloris.html?WT.ad=SlowlorisCaseStudy)
- Home page of SlowHTTPTest (https://github.com/shekyan/slowHttpTest)
- An Attempt at Simulating SlowLoris on LOIC (https://sourceforge.net/projects/loicslow/)
- Blog post explaining the inner workings of Slowloris (https://gkbrk.com/2016/09/about-slowloris/)
