

Forum: [Hack Forums](#)

Thread: [\[FREE\] STRONG DDOS Tools \[Down Websites\]](#)

SpriteZ - September 3, 2011, 8:48 am

Note: Some of these have false positives, if you don't want to risk using them, then DON'T.

JaniDOS: <http://www.mediafire.com/?yxf19r3gyru4372>

Spoiler [\(Click to View\)](#)

<http://www.virustotal.com/file-scan/report.html?id=4e3df2d2c0e0b88130356279d93cbce8f93b0aff0141229e7eb7723c9b2d3889-1315061180#>

HOIC: <http://www.mediafire.com/?t1kejryfrtc8sq>

Spoiler [\(Click to View\)](#)

<http://www.virustotal.com/file-scan/report.html?id=3c9806f8e132917ef85512505fadaca733e5523c271dd2e2a6925ddb9c3d0df0-1315064035>

qSlowloris: <http://www.mediafire.com/?biwxxv8889eja0s>

Spoiler [\(Click to View\)](#)

<http://www.virustotal.com/file-scan/report.html?id=1d8939bfdbb9d6a39d91a2a06c29eb790b6d7b5e96310790d94d7e2c9430e8-1315061859>

HttpAttack: <http://www.mediafire.com/?a9gd8hqj1bgbito>

Spoiler [\(Click to View\)](#)

<http://www.virustotal.com/file-scan/report.html?id=6a1ad41e5d430b75a8c57d64167e1e3fe9c1ef271389062cb3dae45a9bc78269-1312402438>

LOIC: <http://www.mediafire.com/?ezgpvoc0sq0h877>

Spoiler [\(Click to View\)](#)

<http://www.virustotal.com/file-scan/report.html?id=761be0d24961131dad92e35b37d3c42d3ffca05cd1d8738b29ec78cf4f9c625e-1315063296>

Sprut: <http://www.mediafire.com/?mvcajvxgv5aq1ts>

Spoiler [\(Click to View\)](#)

<http://www.virustotal.com/file-scan/report.html?id=626a141437f3ec7414e0a0918d0835ff73e4840f4311c0a31bd22ec1cc4e1287-1315062328>.

You might want to take a look at my other tutorial:

<https://hackforums.net/showthread.php?tid=1686325> if none of these tools work.

iTz Defuzed - September 3, 2011, 10:17 am
thanks for viruz tho bro..thanks alot

Krewella - September 3, 2011, 10:19 am
thanks for these tools mate..also..thanks for scanning them

Rlphy - September 3, 2011, 10:20 am
Thankss even though i never used it ,and isit Virusfree and isit even any good for taking down sitess considering its just a DoS program,and Op your STUPID FOR Relasing it for SOO Manyyy leacherrs,just say Post and PM me Durr

But nicee share though :)

smasherx74 - September 3, 2011, 10:35 am
Thanks for not knowing the difference from DoS and DDoS.

loki` - September 3, 2011, 10:37 am
Thanks for not knowing the difference from DoS and DDoS.

Also thanks for posting public tools.

SpriteZ - September 3, 2011, 10:44 am
(Sep 3, 2011 10:37 AM)?Selena Wrote: [\[CITE\]](#) Thanks for not knowing the difference from DoS and DDoS.

Also thanks for posting public tools.
LOL. I post them as DOS tools - No replies, nobody's interested.
Change it to DDOS and 0mfg err'ybody iz n0w g0nna h4x.

Also, most tools posted here are public, idiot.

V3xD - September 3, 2011, 12:44 pm
All clean uploads.. i tested them all in a VM, good thread!

EvilHeart - September 3, 2011, 12:49 pm
thanks for .. bro..thanks alot
thanks for .. bro..thanks alot

millionstylo - September 3, 2011, 12:52 pm
he dude thx do you have some thing that boot people off xbox?

SpriteZ - September 3, 2011, 1:10 pm
(Sep 3, 2011 12:52 PM)millionstylo Wrote: [\[CITE\]](#) he dude thx do you have some thing that boot people off xbox?
Buy a shell booter from the Marketplace.

Damir - September 4, 2011, 7:38 am
Nice share.
Please post more EXTREME Good Dossers. Thanks Alot!

SaaD - September 4, 2011, 8:21 am
Isnt LOIC a weak tool? It was used by a lot of people attacking the same website at the same time

These are L-DoSing tools not ddos

L-DoSing aka DoSing

Low-rate Denial-of-Service attacks

Recently a new kind of DoS attack, Low-rate Denial-of-Service (LDoS) attack, has been proposed that exploits TCP's retransmission timeout mechanism to reduce TCP throughput without being detected. Compared to traditional flooding based Denial-of-Service attacks, the low-rate DoS attack does not employ a "sledge-hammer" approach of high-rate transmission of packets, and consequently eludes detection.[9] These kinds of attacks are also called shrew attacks, Pulsing DoS (PDoS) attacks, and Reduction of Quality (RoQ) attacks. Recent Publications in low-rate Denial-of-Service (DoS) attacks

The Low-rate DoS (LDoS) attack exploits TCP's slow-time-scale dynamics of retransmission time-out (RTO) mechanisms to reduce TCP throughput. Basically, an attacker can cause a TCP flow to repeatedly enter a RTO state by sending high-rate, but short-duration bursts, and repeating periodically at slower RTO time-scales. The TCP throughput at the attacked node will be significantly reduced while the attacker will have low average rate making it difficult to be detected.[9]

-

DDoS

Distributed attack

Split-arrows.svg

It has been suggested that some portions of this article be split into a new article titled Distributed denial-of-service attack. (September 2011)

A distributed denial of service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods.

Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

A system may also be compromised with a trojan, allowing the attacker to download a zombie agent (or the trojan may contain one). Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts. This scenario primarily concerns systems acting as servers on the web.

Stacheldraht is a classic example of a DDoS tool. It utilizes a layered structure where the attacker uses a client program to connect to handlers, which are compromised systems that issue commands to the zombie agents, which in turn facilitate the DDoS attack. Agents are compromised via the handlers by the attacker, using automated routines to exploit vulnerabilities in programs that accept remote connections running on the targeted remote hosts. Each handler can control up to a thousand agents.[13]

These collections of systems compromisers are known as botnets. DDoS tools like Stacheldraht still use classic DoS attack methods centered on IP spoofing and amplification like smurf attacks and

fraggle attacks (these are also known as bandwidth consumption attacks). SYN floods (also known as resource starvation attacks) may also be used. Newer tools can use DNS servers for DoS purposes. See next section.

Simple attacks such as SYN floods may appear with a wide range of source IP addresses, giving the appearance of a well distributed DoS. These flood attacks do not require completion of the TCP three way handshake and attempt to exhaust the destination SYN queue or the server bandwidth. Because the source IP addresses can be trivially spoofed, an attack could come from a limited set of sources, or may even originate from a single host. Stack enhancements such as syn cookies may be effective mitigation against SYN queue flooding, however complete bandwidth exhaustion may require involvement.[further explanation needed]

Unlike MyDoom's DDoS mechanism, botnets can be turned against any IP address. Script kiddies use them to deny the availability of well known websites to legitimate users.[14] More sophisticated attackers use DDoS tools for the purposes of extortion — even against their business rivals.[15]

It is important to note the difference between a DDoS and DoS attack. If an attacker mounts an attack from a single host it would be classified as a DoS attack. In fact, any attack against availability would be classed as a Denial of Service attack. On the other hand, if an attacker uses many systems to simultaneously launch attacks against a remote host, this would be classified as a DDoS attack.

The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track down and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines.

It should be noted that in some cases a machine may become part of a DDoS attack with the owner's consent. An example of this is the 2010 DDoS attack against major credit card companies by supporters of WikiLeaks. In cases such as this, supporters of a movement (in this case, those opposing the arrest of WikiLeaks founder Julian Assange) choose to download and run DDoS software.

There now you know the difference.

SpriteZ - September 4, 2011, 10:07 am

(Sep 4, 2011 08:26 AM)Ups. Wrote: [\[CITE\]](#) These are L-DoSing tools not ddos

L-DoSing aka DoSing

Low-rate Denial-of-Service attacks

Recently a new kind of DoS attack, Low-rate Denial-of-Service (LDoS) attack, has been proposed that exploits TCP's retransmission timeout mechanism to reduce TCP throughput without being detected. Compared to traditional flooding based Denial-of-Service attacks, the low-rate DoS attack does not employ a "sledge-hammer" approach of high-rate transmission of packets, and consequently eludes detection.[9] These kinds of attacks are also called shrew attacks, Pulsing DoS (PDoS) attacks, and Reduction of Quality (RoQ) attacks. Recent Publications in low-rate Denial-of-Service (DoS) attacks

The Low-rate DoS (LDoS) attack exploits TCP's slow-time-scale dynamics of retransmission

time-out (RTO) mechanisms to reduce TCP throughput. Basically, an attacker can cause a TCP flow to repeatedly enter a RTO state by sending high-rate, but short-duration bursts, and repeating periodically at slower RTO time-scales. The TCP throughput at the attacked node will be significantly reduced while the attacker will have low average rate making it difficult to be detected.[9]

-

DDoS

Distributed attack

Split-arrows.svg

It has been suggested that some portions of this article be split into a new article titled Distributed denial-of-service attack. (September 2011)

A distributed denial of service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods.

Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

A system may also be compromised with a trojan, allowing the attacker to download a zombie agent (or the trojan may contain one). Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts. This scenario primarily concerns systems acting as servers on the web.

Stacheldraht is a classic example of a DDoS tool. It utilizes a layered structure where the attacker uses a client program to connect to handlers, which are compromised systems that issue commands to the zombie agents, which in turn facilitate the DDoS attack. Agents are compromised via the handlers by the attacker, using automated routines to exploit vulnerabilities in programs that accept remote connections running on the targeted remote hosts. Each handler can control up to a thousand agents.[13]

These collections of systems compromisers are known as botnets. DDoS tools like Stacheldraht still use classic DoS attack methods centered on IP spoofing and amplification like smurf attacks and fraggle attacks (these are also known as bandwidth consumption attacks). SYN floods (also known as resource starvation attacks) may also be used. Newer tools can use DNS servers for DoS purposes. See next section.

Simple attacks such as SYN floods may appear with a wide range of source IP addresses, giving the appearance of a well distributed DoS. These flood attacks do not require completion of the TCP three way handshake and attempt to exhaust the destination SYN queue or the server bandwidth. Because the source IP addresses can be trivially spoofed, an attack could come from a limited set of sources, or may even originate from a single host. Stack enhancements such as syn cookies may be effective mitigation against SYN queue flooding, however complete bandwidth exhaustion may require involvement.[further explanation needed]

Unlike MyDoom's DDoS mechanism, botnets can be turned against any IP address. Script kiddies use them to deny the availability of well known websites to legitimate users.[14] More sophisticated attackers use DDoS tools for the purposes of extortion — even against their business rivals.[15]

It is important to note the difference between a DDoS and DoS attack. If an attacker mounts an attack from a single host it would be classified as a DoS attack. In fact, any attack against availability would be classed as a Denial of Service attack. On the other hand, if an attacker uses many systems to simultaneously launch attacks against a remote host, this would be classified as a DDoS attack.

The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track down and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines.

It should be noted that in some cases a machine may become part of a DDoS attack with the owner's consent. An example of this is the 2010 DDoS attack against major credit card companies by supporters of WikiLeaks. In cases such as this, supporters of a movement (in this case, those opposing the arrest of WikiLeaks founder Julian Assange) choose to download and run DDoS software.

There now you know the difference.

I know, but like I posted earlier - People aren't interested if you don't call them 'DDoS' tools.

makoka00 - September 4, 2011, 10:09 am

dont waste your time all this is a shit will not work forst is free second more dos like ddos

SpriteZ - September 4, 2011, 10:13 am

(Sep 4, 2011 10:09 AM)makoka00 Wrote: [\[CITE\]](#) dont waste your time all this is a shit will not work forst is free second more dos like ddos

'All this is a shit'. You're an idiot and I'm glad you're not using them. Kkaithxbai.

chomel - September 4, 2011, 10:58 am

hi nice thanks for the tools.... it very cool... :)

Harmlos - September 4, 2011, 11:09 am

thanks bro i'm downloading now xD

Mfg Harmlos ?

SpriteZ - September 4, 2011, 11:47 am

(Sep 4, 2011 11:09 AM)Harmlos Wrote: [\[CITE\]](#) thanks bro i'm downloading now xD

Mfg Harmlos ?

Thanks. Nice to see not all newbies are ignorant idiots.

Damir - September 4, 2011, 11:52 am

Bro, please add more Strong dossers like QSlowloris.

Much love for this thread!

t0Xin - September 4, 2011, 12:51 pm

thanks, but its not ddos, it's just dos.

SpriteZ - September 4, 2011, 1:42 pm

(Sep 4, 2011 12:51 PM)ToxinHD Wrote: [\[CITE\]](#) thanks, but its not ddos, it's just dos.

Like I've said 3 TIMES IN THIS THREAD; Unless I call them ddos tools, people don't think they work.

.vB - September 4, 2011, 6:59 pm

None of them worked for me so yea, anyways I guess thanks.

SpriteZ - September 4, 2011, 7:23 pm

(Sep 4, 2011 06:59 PM)~Josh~/ / 9-1-01 R.I.P. Wrote: [\[CITE\]](#) None of them worked for me so yea, anyways I guess thanks.

Obviously won't take down some sites. If you came to this thread expecting to take down google, sorry to dissappoint ?.

dat_ - September 4, 2011, 7:34 pm

very nice thread, was always looking for something like this

Galileos_Dream - September 5, 2011, 1:27 pm

I hate to be a downer but in on of the last two norton discovered a trojan

SpriteZ - September 5, 2011, 2:16 pm

(Sep 5, 2011 01:27 PM)Galileos_Dream Wrote: [\[CITE\]](#) I hate to be a downer but in on of the last two norton discovered a trojan

I've posted scan results and multiple people have verified them to be clean. It's detected as either a dos tool or a hack tool.

P.S. Norton sucks.

Kenzix - September 5, 2011, 4:47 pm

This might a veeery dumbass Question, But i'am new in this hacker world.

What does a DDOS exactly do?

zzZSlashZzz - September 5, 2011, 6:39 pm

Which of the above tools are the best in your opinion? As in most effective?

L34rN2H4x - September 5, 2011, 7:35 pm

Thanks for the upload, gonna check'em out.

weedmonster - November 26, 2011, 3:20 pm

thank u op for sharing.respect 1000

Gilbert2 - November 30, 2011, 3:47 pm

thnks, looks cool.. i have something tht will hit people hard on xbox

UNKNOWN WHO - December 1, 2011, 6:53 am

ok this loic sucks it lags up is that gay suck my dick

tjkid - March 16, 2012, 11:40 am

great job dude, thanks for the contribution!

Emyli - March 16, 2012, 12:25 pm

Do I want this..hmm Do I want this..

Seems good. Lots of green reps saying it is okay? Yes. So off I go to download :)

MeTheSlayer - March 16, 2012, 3:12 pm

thank you for these tools bro i appreciate them

Garrett632 - March 16, 2012, 3:38 pm

(Sep 3, 2011 12:52 PM)millionstylo Wrote: [\[CITE\]](#) he dude thx do you have some thing that boot people off xbox?"Cain and abel" I know its a program for that but you can research more about it online now that you know the program.. hope this helps.

Blubex - December 4, 2012, 6:59 pm

(Mar 16, 2012 03:38 PM)Garrett632 Wrote: [\[CITE\]](#) "Cain and abel" I know its a program for that but you can research more about it online now that you know the program.. hope this helps.

Dear God, what has this world come to? Cain and Abel is not a DoS Tool, it is a packet sniffer, password cracker, and some other things I don't know. But, it's not meant for DoSing a network =/

Nicktendo13 - December 4, 2012, 10:07 pm

These seem pretty good, i havent tested many of them extensively tho.