Trinoo

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Trinoo#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Trinoo#searchInput)

|  |  |
| --- | --- |
| **Trinoo** | |
| **Type** | [Botnet](https://en.wikipedia.org/wiki/Botnet) |
| [**Operating system(s)**](https://en.wikipedia.org/wiki/Operating_system)**affected** | [Linux](https://en.wikipedia.org/wiki/Linux), [Solaris](https://en.wikipedia.org/wiki/Solaris_(operating_system)) |
| **Filesize** | 13.6kb |
| **Written in** | [C](https://en.wikipedia.org/wiki/C_(programming_language)) |

The **trinoo** or **trin00** is a set of computer programs to conduct a [DDoS](https://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_attack) attack. It is believed that **trinoo** networks have been set up on thousands of systems on the Internet that have been compromised by remote buffer overrun exploits.[[1]](https://en.wikipedia.org/wiki/Trinoo#cite_note-1)

The first suspected **trinoo** attacks are described in [CERT](https://en.wikipedia.org/wiki/CERT_Coordination_Center) Incident Note 99-04.[[2]](https://en.wikipedia.org/wiki/Trinoo#cite_note-2) A trinoo network has been connected to the February 2000 [distributed denial of service](https://en.wikipedia.org/wiki/Distributed_denial_of_service) attack on the [Yahoo!](https://en.wikipedia.org/wiki/Yahoo!) website.[[3]](https://en.wikipedia.org/wiki/Trinoo#cite_note-3)

Trinoo is famous for allowing attackers to leave a message in a folder called **cry\_baby**. The file is self replicating and is modified on a regular basis as long as port 80 is active.

Trinoo was authored by a teenager from New Orleans who went by the alias phifli.



**Contents**

* [1Using Trinoo](https://en.wikipedia.org/wiki/Trinoo#Using_Trinoo)
  + [1.1Step 1](https://en.wikipedia.org/wiki/Trinoo#Step_1)
  + [1.2Step 2](https://en.wikipedia.org/wiki/Trinoo#Step_2)
  + [1.3Step 3](https://en.wikipedia.org/wiki/Trinoo#Step_3)
* [2See also](https://en.wikipedia.org/wiki/Trinoo#See_also)
* [3References](https://en.wikipedia.org/wiki/Trinoo#References)
* [4External links](https://en.wikipedia.org/wiki/Trinoo#External_links)

Using Trinoo[[edit](https://en.wikipedia.org/w/index.php?title=Trinoo&action=edit&section=1)]

**Step 1**[[edit](https://en.wikipedia.org/w/index.php?title=Trinoo&action=edit&section=2)]

The attacker, using a compromised host, compiles a list of machines that can be compromised. Most of this process is done automatically from the compromised host, because the host stores a mount of information including how to find other hosts to compromise.

**Step 2**[[edit](https://en.wikipedia.org/w/index.php?title=Trinoo&action=edit&section=3)]

As soon as the list of machines that can be compromised has been compiled, scripts are run to compromise them and convert them into the Trinoo Masters or Daemons. One Master can control multiple Daemons. The Daemons are the compromised hosts that launch the actual [UDP floods](https://en.wikipedia.org/wiki/UDP_flood_attack) against the victim machine.

**Step 3**[[edit](https://en.wikipedia.org/w/index.php?title=Trinoo&action=edit&section=4)]

The DDoS attack is launched when the attacker issues a command on the Master hosts. The Masters instruct every Daemon to start a DoS attack against the IP address specified in the command, many DoSs comprise the DDoS attack.

See also[[edit](https://en.wikipedia.org/w/index.php?title=Trinoo&action=edit&section=5)]

* [Stacheldraht](https://en.wikipedia.org/wiki/Stacheldraht)
* [Tribe Flood Network](https://en.wikipedia.org/wiki/Tribe_Flood_Network)
* [High Orbit Ion Cannon](https://en.wikipedia.org/wiki/High_Orbit_Ion_Cannon)
* [Low Orbit Ion Cannon](https://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon)

References[[edit](https://en.wikipedia.org/w/index.php?title=Trinoo&action=edit&section=6)]

* 1. [**^**](https://en.wikipedia.org/wiki/Trinoo#cite_ref-1) <http://staff.washington.edu/dittrich/misc/trinoo.analysis>
  2. [**^**](https://en.wikipedia.org/wiki/Trinoo#cite_ref-2) [*"CERT® Incident Note IN-99-04"*](http://www.cert.org/incident_notes/IN-99-04.html)*.*[*CERT*](https://en.wikipedia.org/wiki/CERT_Coordination_Center)*. April 1999.*[*Archived*](https://web.archive.org/web/20091016021733/http:/www.cert.org/incident_notes/IN-99-04.html)*from the original on October 16, 2009. Retrieved July 27, 2014.*
  3. [**^**](https://en.wikipedia.org/wiki/Trinoo#cite_ref-3) *Sinrod, Eric J.; William P. Reilly (May 2000).*[*"Cyber Crimes: A Practical Approach to the Application of Federal Computer Crime Laws"*](http://www.sinrodlaw.com/CyberCrime.pdf)*(*[*PDF*](https://en.wikipedia.org/wiki/PDF)*235*[*KB*](https://en.wikipedia.org/wiki/Kilobyte)*). Santa Clara Computer and High Technology Law Journal. California:*[*Santa Clara University School of Law*](https://en.wikipedia.org/wiki/Santa_Clara_University_School_of_Law)*.****16****(2): 17.*[*ISSN*](https://en.wikipedia.org/wiki/ISSN_(identifier))[*0882-3383*](https://www.worldcat.org/issn/0882-3383)*. Retrieved 2008-11-04.*

External links[[edit](https://en.wikipedia.org/w/index.php?title=Trinoo&action=edit&section=7)]

* [Trinoo description](https://web.archive.org/web/20051226150250/http:/service1.symantec.com/sarc/sarc.nsf/html/w32.dos.trinoo.html) by [Symantec](https://en.wikipedia.org/wiki/NortonLifeLock)
* [Trinoo Analysis](http://packetstormsecurity.org/distributed/trinoo.analysis.txt) by David Dittrich
* [Trinoo](http://packetstormsecurity.org/distributed/trinoo.tgz) source code