

# Xor DDoS

By Contributors to Wikimedia projects

Published: 2016-03-18 · Archived: 2026-04-05 21:17:32 UTC

From Wikipedia, the free encyclopedia

**XOR DDoS** is a Linux Trojan malware with rootkit capabilities that was used to launch large-scale DDoS attacks. Its name stems from the heavy usage of XOR encryption in both malware and network communication to the C&Cs. It is built for multiple Linux architectures like ARM, x86 and x64. Noteworthy about XOR DDoS is the ability to hide itself with an embedded rootkit component which is obtained by multiple installation steps.<sup>[1]</sup> It was discovered in September 2014 by [MalwareMustDie](#), a [white hat](#) malware research group.<sup>[2][3][4]</sup> From November 2014 it was involved in massive brute force campaign that lasted at least for three months.<sup>[5]</sup>

In order to gain access it launches a brute force attack in order to discover the password to Secure Shell services on Linux.<sup>[6]</sup> Once Secure Shell credentials are acquired and login is successful, it uses root privileges to run a script that downloads and installs XOR DDoS.<sup>[7]</sup> It is believed to be of Asian origin based on its targets, which tend to be located in Asia.<sup>[8]</sup>

- [Application layer DDoS attack](#)
- [BASHLITE](#)
- [Botnet](#)
- [Dendroid \(Malware\)](#)
- [Denial-of-service attack](#)
- [Rootkit](#)
- [Zombie \(computer science\)](#)
- [ZeroAccess botnet](#)

1. ↑ "[Linux DDoS Trojan hiding itself with an embedded rootkit](#)". *Avast*. January 6, 2015. [Archived](#) from the original on September 16, 2025. Retrieved September 7, 2019.
2. ↑ "[MMD-0028-2014 - Linux/XOR.DDoS : Fuzzy reversing a new China ELF](#)". *Malware Must Die!*. [Archived](#) from the original on October 2, 2014. Retrieved September 7, 2019.
3. ↑ Constantin, Lucian (February 6, 2015). "[Sneaky Linux malware comes with sophisticated custom-built rootkit](#)". *PCWorld (From IDG)*. Retrieved February 6, 2015.
4. ↑ Cimpanu, Catalin (September 29, 2015). "[XOR DDoS Botnet Uses Compromised Linux Machines to Launch 150+ Gbps Attacks](#)". *Softpedia News*. Retrieved September 29, 2015.
5. ↑ "[Anatomy of a Brute Force Campaign: The Story of Hee Thai Limited](#)". *Threat Research Blog. FireEye*. [Archived](#) from [the original](#) on March 18, 2015. Retrieved March 18, 2016.
6. ↑ "[New Botnet Hunts for Linux — Launching 20 DDoS Attacks/Day at 150Gbps](#)". *thehackernews.com*. [Archived](#) from the original on March 18, 2016. Retrieved March 18, 2016.

7. <sup>^</sup> ["XOR DDoS Botnet Launching 20 Attacks a Day From Compromised Linux Machines, Says Akamai"](#) (Press release). Cambridge, MA: Reuters. Archived from [the original](#) on March 18, 2016. Retrieved March 18, 2016.
8. <sup>^</sup> ["Threat Advisory: XOR DDoS | DDoS mitigation, YARA, Snort"](#) (PDF). stateoftheinternet.com. Archived from [the original](#) on March 23, 2021. Retrieved March 18, 2016.

---

Source: [https://en.wikipedia.org/wiki/Xor\\_DDoS](https://en.wikipedia.org/wiki/Xor_DDoS)