Xor DDoS

en.wikipedia.org/wiki/Xor_DDoS

Contributors to Wikimedia projects

Jump to navigation Jump to search

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. [1] It was discovered in September 2014 by MalwareMustDie, a white hat malware research group. [2][3][4] From November 2014 it was involved in massive brute force campaign that lasted at least for three months. [5]

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

See also

References

1. ^ *Lucian Constantin (February 6, 2015). "Sneaky Linux malware comes with sophisticated custom-built rootkit". PCWorld (From IDG). Retrieved February 6, 2015.*
2. ^ *Catalin Cimpanu (September 29, 2015). "XOR DDoS Botnet Uses Compromised Linux Machines to Launch 150+ Gbps Attacks". Softpedia News. Retrieved September 29, 2015.*
3. ^ *"Anatomy of a Brute Force Campaign: The Story of Hee Thai Limited « Threat Research Blog | FireEye Inc". Archived from the original on 2015-03-18. Retrieved 2016-03-18.*
4. ^ *"New Botnet Hunts for Linux — Launching 20 DDoS Attacks/Day at 150Gbps". thehackernews.com. Retrieved 2016-03-18.*
5. ^ *Reuters Editorial. "www.reuters.com/article/akamai-ddos-advisory-idUSnPn5TLPMJ+9f+PRN20150929". reuters.com. Archived from the original on 2016-03-18. Retrieved 2016-03-18.*
6. ^ *"Threat Advisory: XOR DDoS | DDoS mitigation, YARA, Snort" (PDF). stateoftheinternet.com. Archived from the original on 2021-03-21. Retrieved 2016-03-18.*

This malware-related article is a stub. You can help Wikipedia by expanding it.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Xor_DDoS&oldid=1066395246"