Cutwail botnet

By Contributors to Wikimedia projects

Published: 2010-04-21 · Archived: 2026-04-06 15:32:11 UTC

From Wikipedia, the free encyclopedia

The **Cutwail botnet**, founded around 2007,[1] is a botnet mostly involved in sending spam e-mails. The bot is typically installed on infected machines by a Trojan component called **Pushdo**.[2] It affects computers running Microsoft Windows.[3]

In June 2009 it was estimated that the Cutwail botnet was the largest botnet in terms of the amount of infected hosts. Security provider MessageLabs estimated that the total size of the botnet was around 1.5 to 2 million individual computers, capable of sending 74 billion spam messages a day, or 51 million every minute, equal to 46.5% of the worldwide spam volume.[2][4]

In February 2010 the botnet's activities were slightly altered when it started a DDoS attack against 300 major sites, including the CIA, FBI, Twitter and PayPal. The reasons for this attack weren't fully understood, and some experts described it as an "accident", mainly due to the lack of damage and disruption, along with the infrequency of the attacks.[5]

In August 2010, researchers from University of California, Santa Barbara and Ruhr University Bochum attempted to take down the botnet, and managed to take offline 20 of the 30 Command and Control servers that the botnet was using.[2]

Cutwail is a fairly simple botnet. The bots connect directly to the command and control server, and receive instructions about the emails they should send. After they are done with their task, the bots report back to the spammer exact statistics on the number of emails that were delivered, and on which and how many errors were reported.[2]

The Cutwail botnet is known as "0bulk Psyche Evolution" in the underground market. Spammers can rent an instance of the botnet for a fee, and use it to send their own spam campaigns. The services offered by the botnet were advertised on the Russian underground forum "spamdot.biz", that was taken down in 2010. As of June 2010, at least 8 different spam groups were using the botnet to deliver junk mail.[2]

- Operation: Bot Roast
- McColo
- Srizbi botnet
- Botnet

1. ^ *Robert Jaques (October 1, 2007). "Angelina Jolie 'nudes' fuel malware spike". V3.co.uk.*

2. ^ Jump up to: ***a*** ***b*** ***c*** ***d*** ***e*** *Brett Stone-Gross; Thorsten Holz; Gianluca Stringhini; Giovanni Vigna (March 29, 2011). "The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns" (PDF). USENIX. Archived from the original (PDF) on July 25, 2014. Retrieved January 25, 2013.*
3. ^ *"Backdoor:Win32/Pushdo.A". Microsoft.*
4. ^ *Harry Waldron (February 2, 2010). "Pushdo Botnet - New DDOS attacks on major web sites". Computer Security News (blog). Archived from the original on 2010-08-16.*
5. ^ *Kirk, Jeremy (2010-02-03). "Pushdo botnet pummels more than 300 Web sites". Itbusiness.ca. Retrieved 2010-04-21.*

- Technical study of the Pushdo trojan
