Cutwail botnet resurfaces in major Facebook scam-paign

Published: 2011-08-30 · Archived: 2026-04-06 00:31:39 UTC

Cutwail – aka Pushdo and Pandex - *Infosecurity* notes, was first seen in 2007 and is a botnet that controls large volume swarms for DDoS attacks and spam email generation.

In June of 2009, it was estimated that Cutwail was the largest botnet in terms of the amount of infected hosts. At the time, MessageLabs estimated that the total size of the botnet was around 1.5 to 2 million individual computers, capable of sending around 74 billion spam messages every day.

In February of last year, the botnet was seen to diversify when it started a DDoS attack against 300 major sites, including the CIA, FBI, Paypal and Twitter.

According to Phil Hay of M86 Software, this latest incarnation of Cutwail is generating spam messages to Facebook users without any attachments.

The message, he says in his latest security posting, arrives as a fake Facebook friend invite notification that appears to be convincing since it is a clone of the real Facebook invite, but with malicious links. The message, notes Hay, doesn't contain any profile photos, and they have omitted the recipient's email address in the fine print at the bottom.

"Clicking the link fetches a web page that contains two ways you can infect yourself. First, there is a link pretending to be an Adobe Flash update where you can download and install malware manually. Second, there is a hidden iframe that loads data from a remote server hosting the Blackhole Exploit Kit, which attempts to automatically exploit vulnerabilities on your system, notably Java", he asserts.

Hay notes that the maware that is downloaded appears to be a Zbot/Zeus variant.

"Impersonation of the big social networks' email notifications is an increasingly common tactic of the spammers. Be wary out there, not everything is as it seems", he says.
