Botnet Malware Gets Refresh

Written by Marco Attard
16 May 2013

According to Dell SecureWorks, Damballa Labs and the Georgia Institute of Technology the Pushdo malware behind the Cutwail spam botnet now has a new communications mechanism making it even more resilient to take down attempts.

Cutwail is one of the oldest and most notorious botnets. Created at around 2007, it infects systems on corporate networks and consumer PCs and uses them to send out vast amounts of spam emails. According to MessageLabs, by 2009 the Cutwail botnet spanned from 1.5 to 2 million individual computers, and was capable of sending out 74 billion spam messages daily, or 46.5% of global spam volume.

Behind Cutwail is the Pushdo malware-- now with a new domain name generation algorithm (DGA) making it even more difficult to detect by intrusion detection and prevention systems and most antimalware technologies. The algorithm mimics legitimate connection attempts to benign websites, confusing signature-based detection systems.

The DGA technique is actually a backup, kicking in use only once the infected machine fails to connect with the primary command-and-control server. Once it starts running, it acts like other backup command-and-control systems used by cybercriminals such as those behind the Zeus banking malware.

"This is a very smart way to defeat generic network signature and sandboxing systems that simply block the network communication observed during the dynamic analysis of the malicious binary," the researchers say.

The team believes India, Iran and Mexico house the largest amount of infected PCs, but several government contractors and military networks in the US are also infected by latest Pushdo variant.

Go Unveiling the Latest Variant of Pushdo