

As Seen On



Friday, February 8, 2008

## Botnet more dangerous than Storm?

By Tom Espiner, ZDNet

Reports are starting to circulate of a botnet being seeded that could be more insidious than Storm, currently the largest and most sophisticated network of compromised computers.

An article in Dark Reading warns of a Trojan that can circumvent most anti-malware products, being aimed at corporate networks. The Trojan and the botnet it is seeking to build has been called "Mayday" by security vendor Damballa, Dark Reading reports.

However, what seems to set this botnet apart is that it can communicate through an organisation's web proxy to download updates.

"MayDay uses a combination of techniques to communicate with its bots, including hijacking browser proxy settings, says Tripp Cox, vice president of engineering for [security company] Damballa," writes Dark Reading. "He says, "It can communicate through an enterprise's secure Web proxy and conduct updates and attack activities" – a unique method for a botnet.

The botnet uses two forms of P2P communications to ensure it can talk to its bots, including [encrypted] Internet Control Message Protocol (ICMP). "This malware is for multiple protocols and is specifically designed to be successful despite whatever security controls might be" in place, Cox says."

I heard whispers of a possible botnet to rival Storm last week, but a quick ring around of security vendors in Europe yielded no information – no-one I spoke to had heard anything.

Since then security vendor Symantec has put out a warning of a Trojan it has called "Daymay", although the risk level it has assigned it is "very low".

I'll keep an eye on this news as it develops.