



Use and distribution of this article is subject to our [Publisher Guidelines](#) whereby the original author's information and copyright must be included.

Current Rating: Not rated

Attackers Connect to Internet through User Computers *by btv raj*

If you think that you are the only person connecting to the Internet using your computer, may you be wrong. A malware named Trojan-Proxy.Win32.Agent.y is on the prowl and like other members of its family, this one too facilitates a remote attacker to access the Internet via a compromised computer, say security experts at MicroWorld Technologies.

Win32.Agent.y comes to your computer when you download many dubious, free applications from the Internet. Drive-by-Download is another mode of propagation for the Trojan as malicious websites force it into computers by exploiting browser vulnerabilities, where all you need to do is to view those websites to get infected.

After finding its way into the computer, the Trojan activates an HTTP Proxy Server on TCP port 12080. It then uses a special configuration program to give a random port number for the proxy. Using it, a remote attacker can connect to different websites and launch nefarious activities like Online Robbery, Identity Theft, Denial of Service attack and Click Fraud Scam.

"A criminal remains at large as long as he manages to keep his identity hidden from the law enforcing agencies," says Rohini Sonawane, Chief Operating Officer of MicroWorld. "This Trojan is made to act as a camouflage mechanism for the attacker to hide his shady activities on the net. Any inquiry to find the origin of an online attack will stop at the compromised PC of a victim, who apparently has no idea what is going on!"

If Trojan-Proxy.Win32.Agent.y is only used for masking IP addresses of attackers, some other Backdoors and Trojans can be employed to take over the computers completely. According to a report published by FBI on Wednesday, over 1 million computer IP addresses are taken over across United States by remote attackers. Because of their widely distributed capabilities, such botnets are a growing threat to national security, national information infrastructure and economy, FBI said.

"Intrusion of any level into one's computer is dangerous as there's no end to it once it begins. With the incremental nature of today's malware, users need to be on their guard while working on computers and more so when connecting to the Internet. Be it office or home users, it's a must to incorporate security practices in one's computer routines. That said, it also calls for protecting your machines with comprehensive security solutions that work on cutting-edge and proactive technologies," views Rohini Sonawane.

MicroWorld

MicroWorld Technologies (www.mwti.net) is the developer of highly advanced AntiVirus, Content Security and Firewall software solutions eScan, MailScan, and eConceal. MicroWorld Winsock Layer (MWL) is the revolutionary technology that powers most of MicroWorld products enabling them to achieve several certifications and awards by some of the most prestigious testing bodies, notable among them being Virus Bulletin, Checkmark, TUCOWS, Red Hat Ready and Novell Ready.

For more information, please visit www.mwti.net