

• [++ GFI LANguard Network Security Scanner 8](#) • [Ad-Aware 2007 Free](#) • [SSL-Explorer 0.2.14.1](#) • [VisualRoute 2007 11.1a](#) • [Password Safe 3.08](#) • [WinSCP 4.0.2](#) • [Lavasoft Personal Firewall 2.0](#) • [J2SSH 0.2.9](#) • [JSch 0.1.33](#) • [TightVNC 1.3.9](#) • [WebScarab 20070504-1631](#) • [ntop 3.3](#) • [ArpAlert 2.0.6](#) • [Integrit 4.1](#) • [MailScanner 4.60.8-1](#) • [pam\\_usb 0.4.1](#) • [NuFw 2.2.0](#) • [strongSwan 4.1.3](#) • [SILC Toolkit 1.1](#) • [FireHOL R5 1.256](#) • [Logwatch 7.3.6](#) • [Another File Integrity Checker 2.10.1](#) • [Tinc 1.0.8](#) • [LockMeBaby 1.12](#) • [1Passwd Password Manager 2.4.6](#) • [Shimo 1.0](#) • [Random Password Generator 1.6.1](#) • [Radmin Assistant 1.0.0](#) • [PDFKey Pro 3.4.1](#) • [MultiAlarm 3.4.2](#) • [Mac GPG 1.4.7](#) • [Little Snitch 1.2.4](#) • [iStumbler 98](#) • [IPSecuritas 3.0rc3](#) • [GlowWorm FW Lite 1.5.3](#) • [SecuBox for Pocket PC 1.2](#) • [Crippin 2.12](#) • [Aircanner Mobile Encrypter 2.9](#) • [Sentry 2020 2.9](#) • [WiFiFoFum 2.1.1](#) • [AirFix 1.0b](#) • [Confidential Notes 1.1](#) • [Aircanner Mobile Firewall 2.4](#) • [WiFi Graph 0.3 RC3](#) • [SignWise Pro 2.52](#) • [eWallet 4.0](#) • [Pocket Warrior 15022003-B](#)

 **ADVISORIES**  **VULNERABILITIES**

• [Gentoo Linux Security Advisory - ClamAV: Multiple Denials of Service \(GLSA 200706-05\)](#) • [Slackware Security Advisory - thunderbird \(SSA:2007-165-01\)](#) • [Mandriva Linux Security Update Advisory - spamassassin \(MDKSA-2007:125\)](#) • [Debian Security Advisory - iceweasel \(DSA 1308-1\)](#) • [SUSE Security Announcement - kernel \(SUSE-SA:2007:035\)](#) • [Apple Security Update - Safari Beta 3.0.1 for Windows \(APPLE-SA-2007-06-14\)](#) • [Elxis CMS 2006.4 banner module sql injection](#) • [Letterman subscriber module XSS vulnerability](#) • [Apache MyFaces Tomahawk JSF Framework Cross-Site Scripting \(XSS\) Vulnerability](#) • [Apache Tomcat XSS vulnerability in Manager](#) • [Apache Tomcat XSS vulnerabilities in the JSP examples](#) • [Apple Safari for Windows feed:// URL Denial of Service Vulnerability](#)



## Trojan horse allows attacker connect to Internet through your computer

Posted on 15.06.2007

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.

If 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.

[ [Virus Center main page](#) ]