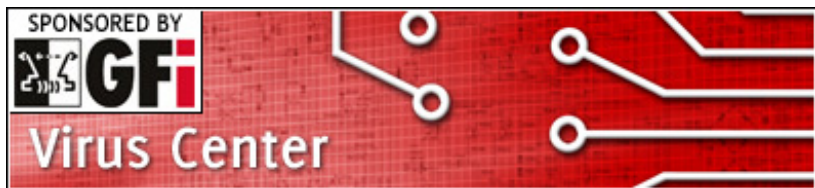


- [++ GFI LANguard Network Security Scanner 8](#) • [Ad-Aware 2007 Free](#) • [SSL-Explorer 0.2.14.1](#) • [VisualRoute 2007 11.1a](#) • [Password Safe 3.08](#) • [WinSCP 4.0.2](#) • [Lavasoft Personal Firewall 2.0](#) • [J2SSH 0.2.9](#) • [JSch 0.1.33](#) • [TightVNC 1.3.9](#) • [WebScarab 20070504-1631](#)
- [Shorewall 3.4.4](#) • [Nmap Parser 1.11](#) • [The Sleuth Kit 2.09](#) • [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](#)
- [TPM Setup 1.0](#) • [The DoorStop X Security Suite 2.0](#) • [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](#)
- [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

- [Debian Security Advisory - evolution \(DSA 1325-1\)](#) • [Trustix Secure Linux Security Advisory - kerberos5 \(2007-0021\)](#) • [Ubuntu Security Notice - linux-restricted-modules-2.6.15/.17/.20 vulnerabilities \(USN-479-1\)](#) • [Debian Security Advisory - hiki \(DSA-1324\)](#) • [Debian Security Advisory - krb5 \(DSA 1323-1 \)](#) • [Debian Security Advisory - wireshark \(DSA 1322-1\)](#)
- [Youtube flagged content age verification bypass](#) • [Google Re-authentication Bypass with SID and LSID cookies](#) • [eTicket version 1.5.5 XSS Attack Vulnerability](#) • [eTicket version 1.5.5 Path Disclosure Vulnerability](#) • [PHP 5.2.3 PHP 4.4.7, htaccess safemode and open_basedir Bypass Vulnerability](#) • [Avaxswf.dll v.1.0.0.1 from Avax Vector software ActiveX Arbitrary Data Write](#)



Poison Ivy can take over your computer

Posted on 26.06.2007

The malware named PoisonIvy.r comes into computers through various online utilities, dubious software programs and movie downloads from infected websites. MicroWorld experts inform that a few cases of the presence of this Trojan have been reported from unprotected computer users in UK and Netherlands.

The Trojan uses a Server component of Poison Ivy, a commonly used Remote Administration Utility. Once inside the computer the malware copies itself into the Windows Root Directory and launches that copy for execution.

PoisonIvy.r gives remote attacker complete access of the compromised computer. Using the Backdoor through TCP channels, an attacker can harvest system information, stop and start processes, take screenshots of the desktop, download files from the net and do much more. The first variant of this Trojan was reported last year, which propagated using documents created in Japanese Text Editor program Ichitaro.

“The shout-out Virus is now a thing of the past,” says Govind Rammurthy, CEO of MicroWorld Technologies. “The in-thing today is a group of stealthier varieties with increasingly furtive nature and modes of infection. And that’s got a lot to do with the radical shift in the motives of today’s malware author as well. She means business and aims to use your computer for either sneaking into organizational networks or to launch all sorts of nefarious activities online”.

[[Virus Center main page](#)]