



SECURITY News

RSS/XML Feeds::

- [Breaking News](#)
- [Security](#)
- [Entrepreneur's Corner](#)
- [More...](#)

SUBSCRIBE TO OUR eNEWSLETTERS:

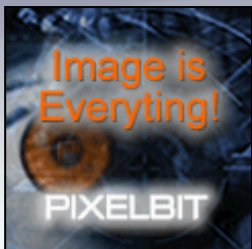
[Quick Register](#)

SEARCH PREVIOUS ARTICLES

SPONSORS:

- Home
- About Us
- Contact Us
- The Glance
- Tech Jobs
- Media Kit
- Great Lakes Financial News
- From PR Newswire
- eNewsletter Signup

- Alternative Energy
- Ann Arbor IT Zone
- Breaking News
- Entrepreneur's Corner
- GLIMA/Automation Alley
- Going Global
- Guest Columns
- Mich Bio
- New Products/Contracts
- Podcast
- Security



Tuesday, June 26, 2007

Poison Ivy, Latest Trojan, Can Seize Your Computer

SOUTHFIELD - A new Trojan on the loose, PoisonIvy.r comes into computers through various online utilities, dubious software programs and movie downloads from infected websites, giving remote attackers complete access to a compromised PC.

MicroWorld experts said a few cases of this Trojan have been reported from unprotected computer users in the United Kingdom 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," said 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."

Users of computers infected with PoisonIvy.r or other Trojans and Backdoors can scan and clean their PCs by downloading the trial version of eScan at [MWTI.Net](#)

Author: Staff Writer
Source: MITechNews.Com

[<< Previous Article](#)

[Printer Friendly](#)

[Next Article>>](#)

Alliance Offices
Shanghai
Beijing

BUTZEL LONG
www.butzel.com