



Poison Ivy on the prowl

Malware makes way into computers through online utilities and hands remote attacker complete access of the compromised computer

Friday, June 29, 2007

Email This Print This Comments RSS

BANGALORE, INDIA: The 1992 movie 'Poison Ivy' was strictly an average fare. But one cannot easily forget 'Ivy', the character played by Drew Barrymore.

Brought into the family of a wealthy couple by their daughter Sylvie, the 'poor' girl Ivy later seduces Sylvie's father, kills her bedridden mother and takes over the family house. A Trojan on the loose does have many things in common with Drew's character, say Security Experts at MicroWorld Technologies.

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".

According to Govind Rammurthy, keeping pace with the fundamental change in today's malware scenario, MicroWorld gives great focus on detecting all sorts of Trojan, Backdoor and Bot varieties. MicroWorld' security solution eScan protects computers with its fast updating remedies for a variety of Spyware and Adware too.

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 MicroWorld's website www.mwti.net.

Related Articles