

eScan Searches and Destroys Two Major Keyloggers

Released by: Manish Katara

Web Site: <http://www.mwti.net>

MicroWorld's eScan successfully detects and removes Keyloggers.



Email: manish@mwti.net

Keywords: [New software release](#), [new product release](#), [antivirus](#), [content security](#), [antispam](#), [spyware detection](#)

Update Date: 3/8/2006 10:59:29 AM

Hits: 3

Description:

eScan from MicroWorld now successfully detects and removes two Keyloggers, namely 'Advanced Keylogger' and 'Family Keylogger'. Both have been highly elusive and hard to defeat for most of the AntiVirus and Spyware removal tools.

A Keylogger runs in the background of computers in invisible mode and records all keystrokes made. This means it can be used to find out everything a person types into his or her computer, including personal letters, business correspondence, user names, passwords and credit card numbers.

The logged keystrokes can then be shipped to an attacker. Once the attacker gets hold of these details he or she can start making purchases online, access sensitive data, sabotage companies or rob bank accounts and do many more. Rootkits and Trojans are known to use Keyloggers extensively.

"While used with Worms and Trojans, malware writers rewrite and alter the source code of these Keyloggers to make it highly unrecognizable. Now that's the biggest challenge. Our algorithms works on a sophisticated behavior and intent analysis to tackle those nasty imposters. This way, we make sure no malware escapes our proactive RADAR." explains Aneesh Paliwal, Security Analyst, MicroWorld, about the technology behind MicroWorld Products.

Two major incidents of online financial theft in recent times were engineered using Keyloggers. They were the Brazilian attack on bank accounts and the money transfer fraud from French bank accounts by Russian hackers. The attack in Brazil, earlier reported by MicroWorld, was quite advanced as Keyloggers transferred funds on their own, in a matter of few seconds after logging on to user accounts. The attack was also special as it bypassed biometric defenses and security gadgets.

"There's been a 65% rise in attacks using Keyloggers in the year 2005 compared to the year before. The worst part is that many computer users are completely unaware of these invisible threats that spy on them day in day out." says Aneesh.

Now, non-users of MicroWorld products can download the free MWAV toolkit from the firm's website to search their computers for malware of this nature.

Contact information:

sales@mwti.net