

# Stealth worm uses anti-debugging technique

*xiando (en)*

A new worm called Atak makes life hard for anti-virus vendors. It checks if it is executed within a sandbox or debugging environment and exits to prevent researchers to get any idea of it's inner workings.

Win32.Atak.A was first discovered and detected 2004-07-12. It is a tipycal mass-mailer worm scans a huge number of different file types for mail addresses and spreads by sending itself as mail attachments.

Anti-virus researchers usually use a virtual environment called a "sandbox" to study how viruses and worms behave. Atak has a feature, or bug, that makes it instantly exit in such environments by comparing the clock to the viruses initial activation date.

I haven't seen such ruses used in a mass mailer in a long time. This piece of code is so sloppy, it's devious, said Mircea Ciubotariu, who analyzed the virus for the anti-virus company BitDefender.

Atak only infects Windows computers used by people foolish enough to open attachments from unknown sources.

The worm is spreading slowly compared to other recent worms and is most anti-virus vendors classify as a low risk. The code itself does pose a threat as this technique is likely to be picked up by other misguided teens with nothing better to do than write evil code.

---

> [Linux Reviews](#) > [News and headlines](#) > [2004 News archive](#) > [July](#) >  
Stealth worm uses anti-debugging technique