Tracking mailclous code with windbg Posted by ictsecurity0 - 14 Feb 2011 - 09:11
Dear all,
Sorry if this is dummy question. Just have the idea that, i success to setup the windbg remote debugging through vmware guest windows xp. Im planning to use windbg to monitoring/tracking the malware activities. my idea is:
windbg (Host)> vmware (guest windows xp running malware)
my question is: 1. possible if we set the break point of malware.exe in guest windows xp? using which command? 2. possible using 'wt' to trace what malware.exe doing?
thanks, from ictsecurity0
Re: tracking malicious code with windbg Posted by Csaba Varszegi - 17 Mar 2012 - 14:24
Hi,
Once you have the kernel debug session established you can use ntsd -d to debug the malware via the connection. You can also use breakin to break into the user mode code.
Cs.