

16 July 2008

By: George Craciun, Security News Editor



New Trojan discovered
by PandaLabs
PandaLabs

[PandaLabs Discovers Trojan in Fake UPS Messages](#)

If you get an unsolicited e-mail from UPS, be cautious

PandaLabs, company that specializes in providing security software solutions, has recently announced that a spam message containing malware has surfaced. The message appears to be sent by parcel delivery company UPS, but in fact it is sent by someone who is maliciously trying to infect your system with a Trojan which PandaLabs named Agent.JEN. Users are advised to be cautious if they receive a message entitled "UPS packet N3621583925" for example. The message claims that a parcel could not be delivered because there is an issue with the recipient's address. In order to recover the parcel which the message says it was sent out on the 1st of July, you are advised to download a .zip file and then print out an invoice. Except that the .zip does not contain any invoices, it contains Agent.JEN.Trojan. Once the Trojan infects a system, it replaces Userinit.exe with userini.exe. You will not notice any changes in your machine's functionality, except that the Userinit.exe file that runs the system interface, explorer.exe and other processes has been swapped with malware. Luis Corrons, Technical Director of PandaLabs comments: "All this effort not to be noticed is in consonance with the current malware dynamic: cyber-crooks are no longer interested in fame or notoriety; they are out to get financial returns as silently as possible. We had seen cyber-crooks use erotic pictures, Christmas or romantic cards, fake movie trailers, etc. as bait to make users run infected files. However, it is not usual to see baits like this one. This clearly indicates that cyber-crooks are trying to use baits that do not raise suspicion to spread their creations." The researchers at PandaLabs have discovered that the Trojan connects to a domain in Russia, which is already known to be used by several banker Trojans. A download query is then forwarded to a German domain, requesting the files Rootkit/Agent.JEP and Adware/AntivirusXP2008. These files considerably increase the risk of your system becoming infected. UPS is currently aware of the situation and has decided to inform its customers via e-mail.