

21 July 2008

By: George Craciun, Security News Editor



Trojan for sale,
guaranteed to run
under the radar
One Man's Blog

[New Trojan Guaranteed to Bypass Detection](#)

A malware product that will do the job without being detected

The Trojan in question has been named Limbo 2, and according to the people who came up with it, the best 10 security software solutions on the market today are not capable of detecting it. Acquiring this malware will set you back about \$1,300, but for that amount of money you will get a software product that is unique, customized to your personal requirements, and guaranteed to run under the radar of most security solutions. "Each variant sold is built anew and has to be customized to incorporate the domain of where all the information is to be sent back to. These are then sold on to websites or botnets to infect individuals," says Prevx, the security company that discovered the threat. What does the Trojan do? Once it manages to infect a system, it goes to work whenever it detects that the user has accessed an online banking service. Not only does it record the regular login info, it also adds spoofed information boxes which ask you to provide additional information in regard to your bank account. All the gathered security credentials are then sent to the person that bought Limbo 2, so that it can be used for whatever malicious purpose that person has in mind. "This is one of the most dangerous Trojans out there at the moment. The strength of this piece of malware lies in its versatility, even if it is recognized up by an anti-virus company it can be changed so as to be invisible again within hours. There are likely to be so many variants out there that they will never all be detected, which is a scary thought as it is designed to steal bank details," says Jacques Erasmus, Director of Malware Research with Prevx. According to Erasmus, this is a very lucrative piece of software, earning the designer of Limbo 2 a few thousand pounds every day. Since it has not yet been detected how the malware propagates, it is safe to assume that the source of infection is a malware spreading site.