

9 August 2006

By: Marius Oiaga, Technology News Editor

## [Internet Explorer BHO Trojan](#)

### *Transmits stolen data via ICMP packets*



Websense Security Labs has announced in a press release that the company has received and analyzed a new Trojan that implements innovative techniques to camouflage its actions. While the keylogger generates traffic containing the information that it has recorded and stolen from a compromised machine, it disguises the data as Internet Control Message Protocol packets. Normally this protocol is reserved for the transmission of erroneous and control messages, router generated unavailability notifications or echo requests from ping utilities. "Websense Security Labs has received a sample of a new phishing Trojan that delivers stolen information back to the attacker via ICMP packets. Upon infection of a victim's computer, the Trojan will install itself as an Internet Explorer Browser Helper Object (BHO). The BHO then waits for the user to post personal information to a monitored website. As this information is entered by the user, it is captured by the BHO and sent back to the attacker. The method of network transport used by the attacker makes this Trojan unique. Typically, keyloggers of this type will send the stolen information back to the attacker via email or HTTP POST, which can appear suspicious. Instead, this Trojan encodes the data with a simple XOR algorithm before placing it into the data section of an ICMP ping packet." explained the company. The ICMP packets containing captured encoded sensitive data bypass administrators and egress filters, as the packet looks masquerade as legitimate traffic. "In our example, we infected a workstation and entered account information into the SSL website of Deutsche Bank. The Trojan BHO captured the information and sent a ping to a malicious remote server. Below you can view the encoded contents of the ICMP data section as well as the actual contents after they were manually decoded," stated Websense.