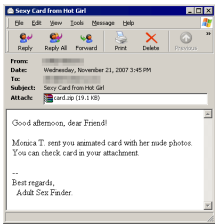


26 November 2007

By: Bogdan Popa, Security and Search Engines Editor



The spam message attempting to trick you to download the attachment
Trend Micro

[Nude Photos? Nope, It's Just a Windows Infection!](#)

Spam message deploying Trojan horses

A new Trojan horse affecting most Windows operating systems was discovered by security vendor Trend Micro which gave a medium damage potential to the threat. TROJ_PUSHDO.AR comes as an email attachment and affects Windows 98, ME, NT, 2000, XP and Server 2003. "This Trojan arrives either as an email attachment to messages spammed by other malware or a malicious user," Trend Micro noted in the security advisory. In addition, it appears that the Trojan can also be downloaded from infected webpage without visitors' approval. Although it might really damage some of the files stored on the hard drives, the most important aspect of this Trojan horse is actually the way it attempts to trick users into downloading it. According to the security company, the email claims it contains nude photos with Monica T. and encourages the receivers to download and decompress the adjacent ZIP archive. "Good afternoon, dear Friend! Monica T. sent you animated card with her nude photos. You can check card in your attachment. Best regards, Adult Sex Finder," the email reads. "It connects to a certain URL to download and execute possibly malicious files. The said file is detected by Trend Micro as TROJ_PANDEX.AR. As a result, malicious routines of the downloaded files may be exhibited on the affected system," Trend Micro described the behavior of the Trojan horse. As far as I can see, TROJ_PUSHDO.AR made a lot of victims all over the world as Trend Micro discovered 352 infected computers in North America, 281 in Europe, 93 in Australia and New Zealand and 24 computers in Asia. Just as usual, it's recommended to keep the installed antivirus solution up-to-date with the latest virus definitions as most security vendors will implement protection for this threat anytime soon. In addition, you should avoid opening untrusted emails and refuse downloading and running attachments coming from unknown sources.