

22 September 2008

By: Lucian Constantin, Web News Editor



New spam campaign targeting airline customers
Wired Blogs

[New Airline e-Ticketing Spam Taking Off](#)

A spam campaign that targets airline customers has caught the attention of security researchers

Researchers from the security company BitDefender came across a new e-mail [scam](#) aimed at spreading malware and claiming to deliver invoices and e-tickets acquired through an online airplane ticket purchase system. As expected, contained in the attached .zip file are several trojan installers.

The e-mails have subjects such as "Your Online Flight Ticket N #####" (where # is a random digit) and they claim to have been sent by major US airline companies and carriers. The body of the e-mails informs the users that they've used a "Buy airplane ticket Online" service on the website of an airline company.

In order to be more believable, a login (the user's e-mail address) and password are provided as well as instructions on how to use the supposed ticket that is attached in the .zip file. It even goes as far as to provide a marketing reminder that a discount is available when tickets are bought through this so-called service.

The BitDefender researchers speculate that the group responsible for this spam campaign is the same one that launched the Jet Blue Airways scam back in July. "Instead of the attack spoofing Jet Blue Airways identity reported in July, this new round of attacks targets the major U.S. air carriers as well as other operators including cardinal points within their names." This makes researchers think that the attackers are trying to target the start of the school year as well as people who are planning a late vacation.

The specific threats spread by these e-mails have been identified as Trojan.Spy.Zbot.KJ and Trojan.Spy.Wsnpoem.HA as well as Trojan.Injector.CH. The BitDefender advisory notes that the same malicious applications have been used in attacks targeting customers of overnight delivery companies. Upon installation, the applications run hidden in the background and they are uploading gathered sensitive information to remote servers as well as opening exceptions in the Windows firewall and listening to specific ports for commands from the attackers. It is also pointed out that the trojans attempt to download files from Russian servers.

"Users should be aware that without the appropriate security solution the integrity of their systems is at an extremely high risk," said Sorin Ducea, head of BitDefender Antimalware Research. "The Trojans this new malware distribution campaign delivers and the high rate of infections prove once again not just the cybercriminals' ingenuity, but also the lack of interest the users show in terms of systems' defense and sensitive data protection," he added.

While certainly more believable than the last [spam campaigns](#) we reported, regarding a fake Obama adult video, a UK nuclear explosion and threats of suspended Internet access coming from a fictional ISP Consortium, these spam e-mails also do a better job when it comes to the English spelling. Except for the "Dear Gentlemen," addressed to single individuals and the "print it on a color printed" instead of printer, the messages are quite well formulated, which makes them even more dangerous in tricking users regarding their authenticity.