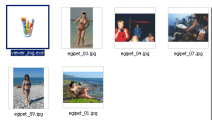


26 November 2007

By: Bogdan Popa, Security and Search Engines Editor



The files included in the attachment
F-Secure

[Have You Seen Anita's Egyptian Vacation Photos?](#)

It's only spam

A new spam campaign is currently in progress attempting to install several infected files on users' computer by tricking them to download and access attached imagery. But this new unsolicited email is quite different from other spam campaigns because the attached archive really contains several photos including (keep it in mind) an infected file. Here's how it works: a spam message reaches your inbox, claiming that it contains some photos with Anita and his vacation in Egypt. The attached file is a ZIP archive which contains several pictures and an executable file which apparently seems to be MS Paint. Once started, the application downloads several infected files without users' approval. The entire exploitation is done in background so you need some security tools to notice this. "Hi Michael and Simona, there are my pictures from my Egypt vacation. Call me when you come. Best regards," Anita," the spam message reads. The attachment is named as "my_holiday_in_egypt.zip" while the attached executable file seems to be a Russian version of MS Paint. "Of course, this is just a bluff. In the background it's dropping and executing a variant of the LdPinch data-stealing trojan. Let's see. It loads up a Russian version of pbrush.exe. The images are named "egipet.jpg" - Egipet is the Russian spelling of Egypt. And LdPinch is Russian malware," the F-Secure team, the one that discovered this spam campaign wrote today. As you probably know, you're advised to avoid opening emails coming from untrusted sources as well as refuse downloading attachments included in unknown messages. In addition, you should keep your antivirus up-to-date with the latest virus definitions because it could detect the threats included in the attachments and block them before they attempt to deploy more infections on the affected systems.