Sality & Stuxnet - not such a strange coincidence

Kaspersky Lab announces the publication of its *Monthly Malware Statistics* for September 2010. The change in seasons brought with it advances in the Sality virus and an increase in the number of adware programs on the web.

According to Kaspersky Lab statistics, a new variant of the notorious polymorphic Sality virus, dubbed 'bh', was found to be particularly widespread on users' computers. A newcomer to the ranking, Sality.bh claimed eleventh position and spread with the help of Trojan-Dropper.Win32.Sality.cx which uses vulnerability in Windows LNK files.

This is the first detected zero-day vulnerability to be used by the now infamous Stuxnet worm. This same vulnerability was exploited by Trojan-Dropper.Win32.Sality.r back in August. The geographical distribution of the droppers in question mirrors that of the Stuxnet worm, both of them appearing most prolifically in India, followed by Vietnam and then Russia.

Don't encourage cybercriminals - update!

"Cybercriminals are usually very quick to release exploits when new vulnerabilities are discovered. The fact that huge numbers of users fail to update their software on a regular basis only encourages them." commented Vyacheslav Zakorzhevsky, senior virus analyst and author of the review.

An advertising theme is also evident in the second ranking of web threats - for the first time the number of adware programs was equal to the number of exploits, which remain popular with cybercriminals. A total of seven AdWare.Win32 programs made it into this month's Top Twenty ranking. These types of adware are more annoying than harmful. Their main aim is to attract the attention of users with advertising banners that are integrated into conventional software. Although they are generally harmless, such programs do slow down the operating speed of a computer.

Something of a curiosity in September's web-borne threat ranking is the newcomer Exploit.SWF.Agent.du which is a Flash file. Until now, it's been relatively rare to see vulnerabilities in Flash technology being exploited.

The full version of the September malware ranking from Kaspersky Lab is available at www.securelist.com/en