

Sophos finds 9500 web pages hosting malicious code every day

By Wolfgang Gruener, Friday, June 01, 2007

Boston (MA) – Sophos has published its security report for May and said that malicious code is spreading through the web at an accelerated pace.

The company claims that it has identified an average of 9500 web pages including [malware](#) in May – which is about 1000 pages more than Sophos identified on an average day in April. Including websites that temporarily hosted websites, the security firm identified 304,000 malware sites in May, a spokesperson told TG Daily.

The company estimates that there are currently about 450,000 websites that are infected with malicious code, with the number of potential sites [hosting](#) malware hovering around 750,000, we were told.

The Mal/Iframe threat, which injects [malicious code](#) onto legitimate web pages, remained on the top of Sophos' threat ranking, capturing a 65.5% share. JS/EnclFra and Troj/Decdec followed with 6.9% and 6.5%, respectively. All other top-10 threats, including Troj/Fujif, Troj/lfradv, VBS/Redlof, Mal/ObfJS, Troj/PSyme, VBS/Roor and VBS/Soraci, are listed with a share of less than 4%.

"Each month, we are seeing an increase in attacks spreading over the internet, and they continue to cause problems for organizations," said Ron O'Brien, a [security](#) analyst at Sophos. "Malicious sites do not need to host malware to be dangerous. Our Labs are also seeing and blocking access to 600 new phishing pages each day."

China is still the top-ranked country when it comes to the origin of malware [websites](#). China has a share of 53.2%, followed by the U.S. with 27.4% and Germany with 5.1%.

New on the list is Thailand in position #5 and a share of 1.1%. Sophos noted that "many" of the infected web pages hosted in Thailand are actually on government websites. "It's a bit worrisome that malware is being found even on legitimate government websites," O'Brien said. "It goes to show that any organization can be hit if it is not adequately protected. For those who surf the web, they need to make sure that their anti-virus and security patches are always up-to-date, and they should talk to their administrator or ISP about blocking access to infected websites."