

28 November 2007

By: Bogdan Popa, Security and Search Engines Editor



The avalanche of words published by the attackers
Adam Thomas of the Malware Research Team

God, These Google Hackers Are Smart!

Ingenious method to attract a considerable number of victims

Yesterday, the folks at security company Sunbelt confirmed that the latest trend in today's web attacks is related to Google, as more hackers attempt to get a higher PageRank in Google and bring more potential victims to their websites. Usually, they manage to do so by hacking other websites and placing hidden links inside them, but it seems that another ingenious technique is being used now. Adam Thomas, of the Malware Research Team, wrote on the Sunbelt Blog that more and more attackers create huge websites containing all the words you may know and that may be used by a consumer on a search engine. This is not something new, because these websites are already prohibited by most search engine providers, as they represent search engine spam, and are removed as soon as they are discovered. But, it appears that today's malicious pages have a IFRAME link attempting to break into the vulnerable systems and infect the computers. "For months now, our Research Team has monitored a network of bots whose sole purpose is to post spam links and relevant keywords into online forms (typically comment forms and bulletin board forums). This network, combined with thousands of pages such as the two seen above, have given the attackers very good (if not top) search engine position for various search terms," Adam Thomas wrote. The malware supposed to be installed on the vulnerable users' computers was identified as Scam.lwin. This is another smart component of the entire exploit, because the threat attempts to use the victim's system to generate money for the attacker through the online advertising platforms. "With Scam.lwin, the victim's computer is used to generate income for the attacker in a pay-per-click affiliate program by transmitting false clicks to the attacker's URLs without the user's knowledge. The infected Scam.lwin files are not ordinarily visible to the user. The files are executed and run silently in the background when the user starts the computer and/or connects to the internet", the security expert continued.