New search engine to track down viruses

July 25 2006

The hundreds of thousands of computer users whose PCs have been torn asunder by viruses could now have a new weapon in their arsenal against online attacks. A new search engine has been launched that will exclusively hunt down the pesky malware that make the lives of so many Net users a misery. Using a simple Google search, users will able to enter keywords into the Malware Search engine and track down live malware samples.

Malware -- the term is an amalgamation of "malicious" and "software" -- is the irritating software designed specifically to infiltrate and damage a computer system, and includes such beasties as Trojan horses, spyware, viruses and worms.

The engine has been developed by HD Moore, a well-respected software engineer who works as the director of security research at the Austin-based BreakingPoint Systems and who was responsible for creating the Metasploit hacking tool and the MoBB (Month of Browser Bugs) project. According to an interview in eWEEK, Moore was partly motivated to create by the announcement that Websense Security Labs were using the Google SOAP (Simple Object Access Protocol) Search API to find dangerous .exe files, or executables, that were sitting on Web servers. Although Google SOAP is free for anyone to use, Websense were only sharing the results of searches on private security mailing lists. Moore decided to take a more altruistic approach and, together with researchers from the Offensive Computing project, created Malware Search using open-source programs.

The engine would be simplicity itself to use -- in a user-friendly Web interface, Internet users just need to enter the names of the malware they want tracked down, such as "Bagle," "SoBig" or "MyDoom." The engine will then hunt through hundreds of thousands of Web sites to track down the ones that are hosting the malicious executables. The engine's site closely resembles Google's design, and as with Google, will bring up search results of the Web sites that were purposefully or inadvertently hosting the malware searched for. Broader searches can also be performed using more general search-terms such as "e-mail" or "Trojan." So far, the engine is limited to Google-based queries, but this may be expanded at some stage in the future.

Malware Search differs from other similar programs such as Netsense in that it is open source, making it more freely and widely available than its predecessors. Members of many of the online software interest forums such as Slashdot showed eager encouragement for the engine and saw potential uses in both the workplace and at home. IT managers for non-technology companies would be able to determine if any glitches in the behavior of their internal networks was due to malware sitting in one of the company's computers. At the broader level, Internet hosting providers would be able to keep tabs on their customers to see if any servers were hosting malware, and let the servers' operators know that their sites may have been breached. As one poster on Slashdot enthused, "The combination of this system and using Google for internal searches could make Google a sudden major competitor in the anti-malware campaign."

The program identifies specific malware without the Google application programming interface, using instead code string "fingerprints" from malware samples that the Malware Search programmers already have access to. According to Moore, the engine has already been programmed with 300 malware signatures, and there are plans to add a further 6,000 in a future bug update.

On the Net: metasploit.com/research/misc/mwsearch/index.html