Title:
How does proactive spyware research work

Word Count:
247

Summary:
Phileas system is an automated spyware detection bot network that crawls the Web looking for potentially dangerous application code. This article explains in brief how this proactive spyware research approach works.

Keywords:
phileas spyware network bot

Article Body:
Phileas' purpose is to detect spyware programs before they reach unaware PC users that surf the Internet. This proactive spyware research approach is to revolutionise the way how internet security companies do their research on newly identified threats, malware and spyware available on the Web.
Phileas doesn't follow the standard report-research pattern when it comes to finding new ways to tackle malicious software. To the contrary, it crawls the Web and updates the threat database automatically by transferring information about its findings to Webroot's central unit. The information is being gathered via sophisticated Phileas bot network that crawls the Internet 24/7 sends results to Webroot for processing.

Phileas can detect malicious code, exploits and suspicious applications using its detection algorithms - Phileas bots scan Web sites for forged URLs, manipulated scripts and for susItpicious applications. If they come across a potentially dangerous site, the security researchers target the website or application scrutinizing the information.

The bot network identifies known threats and forwards information about unknown suspicious programs for processing to Webroot. This data is being used to create spyware definitions.

Webroot's application is collecting gathering data related to exploits and malicious code that are being used to transport spyware on the Internet and about the spyware's originator.

Historically, anti-spyware vendors had relied on the Internet user community's

reports about new spyware. Phileas relies on a proactive approach that aims at collecting research data and information about new flaws and exploits by actively scanning the Web for potentially malicious code.