



# RGcrawler Data Product Brochure

Today, about two-thirds of all PCs are believed to have some form of malware infection. Data from Forrester Research shows that 17 percent of businesses said their systems have suffered from spyware this year, and the firm expects that number to climb to 25 percent within the next 12 months. In almost all cases, malware infections result from a user voluntarily downloading and installing software (executable programs) from the Internet that containing malware. Malware can also make its way onto a computer via file sharing.

What's more, today's malware is more malicious and dangerous than ever. For example, adding keyloggers, DLL injections (process hijacking), calling out over the network, or changing computer privileges are all commonplace tactics. Malware programs can also take control of a PC, using it as a zombie or bot to relay spam, store illicit data or conduct denial of service attacks. Traditional antivirus software that works well for virus detection protects users only from discovered threats or identified malware, and is therefore inadequate to keep pace with the ever-morphing forms of malware and zero-day threats.

## RGcrawler Data: Every Executable On the Internet Analyzed

RGcrawler data is created from Robot Genius' patent-pending technology, the industry's first automated malware web crawler. It provides the most effective process for identifying the exact location of all malware on the Internet by identifying the full URL path to the malware.

The Robot Genius web crawler locates all Windows executable programs on the web, including ActiveX or cab files, applets and zip files, and downloads them to a local multi-terabyte storage database for testing. Robot Genius test bed machines run patent-pending software to install each Windows executable program and test whether it is malware. This process creates the RGcrawler data,

the most comprehensive 'block list' of exact malware URLs malware, with a near-zero false positive detection rate.

RGcrawler data is created from patent-pending automated processes for discovering, downloading and testing every executable on the Internet, without human intervention. The data is compiled with groundbreaking speed and accuracy, delivering results for zero-day threat protection.

## RGcrawler Data Applications

RGcrawler data has three common applications. Search Engines and Internet Service Providers use the data to mark up browser search results by adding malware safety ratings, creating a safer browsing environment for users. Desktop security software solution providers use it to build a more comprehensive malware block list to strengthen their existing security software solutions and provide near zero-day threat protection. And Firewall/Gateway vendors use the data to increase the accuracy of their block lists used to block malicious URLs, delivering a safer Internet environment for their customers.

## A Comprehensive Solution

When combined with Robot Genius products RGguard, a lightweight browser plug-in enhancement, and Spyberus, an anti-malware desktop security client that detects and remediates malware from users PCs, RGcrawler data provides the most comprehensive prevention, detection, and remediation against malicious threats.

## Found Out More

For more information about Spyberus and other products from Robot Genius, visit [www.robotgenius.net](http://www.robotgenius.net)

## Key Benefits

RGcrawler data turns the tables on malware producers by providing:

- A comprehensive database covering all executables available on the Internet.
- A valuable and desired 'block list' of all URLs which point to malware.
- An exact 'allow list' of safe executables.
- Zero-day threat protection against all types of malware.
- The fastest, most powerful, fully automated method for discovering all malicious executables on the Internet.

