Webroot® Real-Time Anti-Phishing Service

Overview

» Phishing is the most prevalent type of Internet security attack, and is becoming cybercriminals’ preferred way to breach networks.

» Static anti-phishing blacklists, even if updated hourly, are often ineffective against the dynamic nature of today’s phishing attacks.

» The Webroot Real-time Anti-Phishing Service allows partners to provide significantly better protection against zero-hour phishing threats, disguised redirection, and newly hijacked websites.
  – Not delivered via a URL blacklist or feed
  – Real-time site analysis at the exact moment of the request
  – Live site analysis in under a second

The Webroot Real-time Anti-Phishing Service allows partners to provide significantly better protection than static phishing blacklists against zero-hour phishing threats. Backed by the most advanced machine learning technology in the industry and real-time Webroot® Intelligence Network™ (WIN) cloud services, this anti-phishing protection provides superior security against one of the most pervasive threats facing businesses today. Vendors of anti-fraud services, email security, email infrastructure, social media, SMS, Web browsers, endpoint security, DNS, perimeter security appliances, search engines, mobile carriers, mobile apps, and others now have a better solution with which to protect their customers.

In a recent Webroot survey of IT Directors conducted in the USA and the UK, 55% of respondents reported the number one Internet security breach was phishing.¹ Phishing and spear phishing is now targeted at businesses of all sizes and is rapidly becoming the preferred way cybercriminals breach networks. Phishing attacks are now so sophisticated, they often fool even IT security professionals. In a recent RSA study, the estimated cost to the global economy in fraud damages from phishing attacks increased to $1.5 billion (22%) between 2011 and 2012.²

Static anti-phishing blacklists, even if updated hourly, are often ineffective against today’s phishing attacks. Real-time URL validation is the only truly effective protection against zero-hour attacks, disguised redirection, and recently hijacked websites.

The new Webroot Real-Time Anti-Phishing Service protects users by ensuring they visit only the websites they intend to interact with. Sites are verified at the time of the request to ensure they are genuine and safe.

¹Webroot Web Security Survey, December 2012
²RSA “The Year in Phishing”, January 2013
STOPPING PHISHING ATTACKS IN THEIR TRACKS

The Webroot Real-Time Anti-Phishing Service identifies and stops advanced phishing attacks, helping prevent security breaches and data losses. The service leverages Webroot’s advanced machine learning and content classification to automate the detection of phishing sites. In extensive testing, this new approach detects phishing sites three to five days ahead of the competition—a major breakthrough in the defense against phishing attacks. These sites are typically live very briefly to avoid discovery by other anti-phishing technologies, so early detection is critical.

The service crawls and evaluates requested URLs in milliseconds using hundreds of site attributes, as well as external factors associated with the site from WIN™ cloud security services. These include domain reputation, IP reputation, how long the site has been in existence, recent threat history, etc. The service returns a risk score for each requested URL. Multi-lingual human web analysts evaluate any edge cases. Any human determinations are fed back into the machine learning model to continually refine results for maximum accuracy.

HOW THE TECHNOLOGY IS UTILIZED WITH PARTNERS

Webroot provides both a RESTful Web service as well as a software development kit (SDK). Technology partners can incorporate the Webroot Real-Time Anti-Phishing Service into their own solutions, including:

» Network appliances to improve Web security
» Anti-fraud services to identify new zero-hour threats
» Web browsers and plugins to provide safe browsing
» Email filtering software and endpoint security products
» Filtering user-generated content in social networks, blogs and messaging apps

Whenever users access the Internet, the Webroot Real-Time Anti-Phishing service can protect them from accidentally compromising their online accounts or downloading threats or unwanted applications from malicious sites.

About Webroot

Webroot is bringing the power of cloud-based software-as-a-service (SaaS) to Internet security with its suite of Webroot SecureAnywhere® offerings for consumers and businesses, as well as offering its security intelligence solutions to cybersecurity organizations, such as Palo Alto Networks, F5 Networks, Corea, Juniper, and others. Founded in 1997 and headquartered in Colorado, Webroot is the largest privately held Internet security organization based in the United States—operating globally across North America, Europe and the Asia Pacific region. For more information on our products, services and security visit: www.webroot.com, the Webroot Threat Blog: http://blog.webroot.com or Webroot on Twitter: http://twitter.com/webroot.

©2013 Webroot Inc. All rights reserved. Webroot, SecureAnywhere, Webroot SecureAnywhere, Webroot Intelligence Network and WIN are trademarks or registered trademarks of Webroot Inc. in the United States and/or other countries. All other trademarks are properties of their respective owners.