WEBROOT
Smarter Cybersecurity™

BrightCloud®
Real-Time Anti-Phishing Service

Accurate, next-generation, real-time protection against phishing attacks

Overview

» The most dangerous phishing sites are short-lived, living minutes or hours, not days

» Static phishing lists are too slow to keep up with the pace of today's attacks

» The BrightCloud® Real-Time Anti-Phishing Service provides security vendors with the ability to leverage time-of-need site scans to prevent users from visiting malicious sites

The internet is littered with millions of new phishing sites that appear and disappear in the blink of an eye. To protect your customers from today's highly targeted attacks, detection, detection times must be measured in milliseconds, not days. The BrightCloud Real-Time Anti-Phishing Service enables partners to provide significantly better protection against zero-hour phishing threats than static or crowd-sourced phishing blacklists. Backed by the most advanced machine learning technology in the industry and the Webroot® Threat Intelligence Platform, the service provides best in class protection against one of the most pervasive threats facing businesses and end users 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 comprehensive solution with which to protect their customers.

Phishing and spear phishing attacks are now aimed at businesses of all sizes, and are a preferred method cybercriminals use to breach networks. Analysis of phishing attempts by the Webroot® Threat Intelligence Platform shows that during 2017, almost 100% of phishing URLs used domains typically associated with benign activity, making it much harder to recognize the URLs as malicious.[1] Phishing attacks are so sophisticated, they often fool IT security professionals. Static anti-phishing blacklists, even if updated hourly, are often ineffective against today's phishing attacks. By the time blacklists are published, they are often three to five days old.

Webroot analysis showed that in 2017, the majority of phishing sites' life spans ranged from as low as 15 minutes to under 15 hours, with an average active time of 4-8 hours.[1] Real-time URL validation is the only truly effective protection against zero-hour attacks, disguised redirection, and recently hijacked websites. The BrightCloud® 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 legitimate and safe.

Stopping Phishing Attacks in Their Tracks

The BrightCloud Real-Time Anti-Phishing Service crawls potential phishing links and determines their risk level in real time, at the moment of a web request, providing the most effective protection possible against zero-hour phishing attacks. The service helps prevent security breaches and data loss by leveraging advanced machine learning and content classification to automate phishing detection.

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 detection 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. This includes correlated intelligence from the contextual analysis engine, such as web 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.

Most phishing sites are live for less than 15 hours.[1]

[1] Webroot 2018 Threat Report, March 2018

Add-on BrightCloud Threat Insights for the Real-Time Anti-Phishing Service provide supplementary information on phishing URLs. This includes:

» Identifying the target of the phishing site so that users can identify patterns in attacks and focus their analysis

» A snapshot of the phishing site when it was live to enable customers to see what the site looked like

» Additional data on the URL used for the phishing attack

» Searching for phishing URLs that attempt to imitate a specific brand or website

Partner Benefits

» **Differentiate yourself from your competition**
Offer highly accurate, next-generation, real-time protection against phishing attacks

» **Leverage the Webroot® Threat Intelligence Platform**
Harness the world's most powerful cloud-based security analysis engine

» **Easy to integrate, easy to use**
Simple integration into your solution via RESTful API and an SDK

» **Minimal impact on user experience**
Sites are scanned in real-time to provide advanced protection with minimal user interruption

BrightCloud Real-Time Anti-Phishing Service in Action

Whenever users access the internet, the BrightCloud Real-Time Anti-Phishing Service can protect them from accidentally compromising their accounts or picking up malware or ransomware from malicious sites. Additionally, this service can be integrated to:

» Improve web security for network appliances

» Identify new zero-hour threats for anti-fraud services

» Provide safe web browsers and plugins

» Enhance email filtering software and endpoint security products

» Filter user generated content in social networks, blogs, and messaging apps

Integration Options

Webroot provides a RESTful web service, as well as an SDK, allowing partners to incorporate the BrightCloud Real-Time Anti-Phishing Service into their own solutions with ease. Additionally, this service combines with existing security solutions through the same SDK as other BrightCloud services, making integration as simple and straightforward as possible.

About Webroot

Webroot was the first to harness the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers and small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900