Keeping Bots Out

Bot Mitigation Datasheet

Almost all modern web attacks include the use of bots to interact with the targeted domain. Without a reliable method for identifying and excluding bots, your site will be vulnerable to pen tests (leading to intrusions and breaches), defacements, DoS/DDoS attacks, content scraping, fuzzing, brute force login attempts, and many other forms of attack.

Conventional Approaches Are Inadequate

Modern bots have become quite sophisticated. Some can credibly mimic human web visitors, sending keystrokes, mouse movements, and mouse click events to the targeted site. Unfortunately, many web security products have not kept up with these advances, and they use obsolete detection methods, such as inspecting the incoming requests for known bot signatures. However, most of these detection techniques can be avoided by spoofing and other forms of obfuscation.

Next-Generation Bot Mitigation

Reblaze has pioneered several new methods for detecting and excluding unwanted bots. Legacy techniques like request inspection are still used, but Reblaze attacks the problem from multiple angles simultaneously. See the sidebar to the right for more details.

Using Big Data and Machine Learning to Defeat Bots

Reblaze maintains a massive dataset in the global cloud: petabytes of user behavior data, not only from the domain being protected, but of all the traffic the platform has ever encountered globally. Reblaze can instantly marshals years of data and analytics against any potentially hostile traffic source, whether bot or human, instantly recognizing if that user's behavior is legitimate or not.

Additionally, Reblaze uses machine learning to learn and develop over time. Even as hackers develop new attack techniques, the platform becomes more sophisticated, always adapting to the ever-changing Internet environment.

The Superior Cloud Solution

Along with its proprietary bot-detection technologies, Reblaze gives you many other advantages over competing "cloud" security products. For example, Reblaze provides the most powerful ACL capabilities in the industry. Also, other cloud solutions have a serious flaw; they require you to share resources with their other users, which introduces co-location vulnerabilities. Conversely, Reblaze deploys a unique private cloud around your network—an entire dedicated stack (including DNS servers, load balancers, logs, database, etc.) for your exclusive use alone.

ADVANCED BOT MITIGATION

Reblaze uses visitor behavior, challenges, and honeypots to detect even advanced bots powered by full-stack browsers such as Webkit, Chromium/V8, and IE-WebBrowserControl that bypass traditional bot detection methods.

While other security solutions are signature-based, Reblaze goes much farther. Along with comparing incoming requests to known bot signatures, it also profiles the requestors according to their geographic location, originating network, anonymizer and proxy usage, and many other factors that help to characterize the intent of each traffic source.

Moreover, Reblaze tracks and analyzes requestor behavior over time, including traffic parameters, pace, diversity of MIME types, and more. Reblaze leverages Big Data and the computing capacity of the global cloud to instantly and accurately identify hostile behavior patterns. If at any time a user begins to display hostile intent, that IP address is instantly banned for a configurable length of time.

Reblaze identifies and blocks pen tests, scrapers, data thieves, and other forms of malicious bots, along with other web attacks. This all occurs automatically, with no user intervention required. Reblaze is a PCI DSS Certified Level 1 Service Provider.

How It Works

Reblaze is always on, and always protecting your web assets. Attack detection and mitigation occur 24/7, automatically.

All incoming traffic passes through your private cloud for scrubbing, before being allowed to access your network. Dynamic DNS allocation prevents attackers from reaching (or even finding) the targeted data centers. Meanwhile, legitimate traffic is allowed through as usual, with little if any additional latency. Indeed, most Reblaze-shielded sites are more responsive to their users than they were previously, thanks to Reblaze's global load balancing and CDN integration.

Network reconnaissance attempts are automatically detected and denied. This mitigates many attacks before they even begin.

Multidimensional analysis accurately identifies hostile traffic. Reblaze analyzes multiple traffic dimensions, including content, rate (the throughput of packets, requests, messages, etc.), and ratio (a per-protocol assessment of messages, packets, requests, and data types). Malicious packets are precisely identified, with a minimum of false positives.

Hostile traffic is blocked, and its source is banned. Reblaze tracks the amount of hostile traffic originating from each IP address. When an IP exceeds specified thresholds, that address is banned as a traffic source for a configurable amount of time. Reblaze does this automatically, with no user intervention required.

Bandwidth scales automatically as needed. As resource requirements increase, Reblaze automatically brings more bandwidth online. Reblaze can access higher levels of bandwidth than even many ISPs, limited only by the capacity of the global cloud.

Reblaze learns and adapts to changing traffic patterns. This maintains a high level of accuracy for attack detection. In addition, this saves the user from the usual overhead and ongoing manual fine-tuning required by standard security products.

Immediate upgrades protect against new forms of attack. Your Reblaze deployment is maintained and upgraded automatically by Reblaze's team of security experts. Even as new attack vectors arise, Reblaze is updated immediately. You always have the latest protection against the full breadth of Internet threats.

About Reblaze

Reblaze is the comprehensive, cloud-based, robust protective shield for your web assets. Core technologies include: WAF/IPS, Multilayer DoS/DDoS protection (network, transport, and application), Anti-Scraping, High-level ACL, Advanced Human Detection and Bot Mitigation, Advanced Management Console, and Real-time Traffic Analysis. Added value services include: Layer 7 Load Balancing, Global Secured CDN, and a complete DNS solution. www.Reblaze.com. Contact: hello@reblaze.com. U.K. office: info@datashepherd.co.uk, (0161) 711 0103. International: +972 (73) 252-7007. U.S./Canada office: Reblaze Technologies, 940 Stewart Dr., Sunnyvale, CA 94085. (408) 907-7712.

OTHER BENEFITS

FAST DEPLOYMENT

Shielding your network with Reblaze requires only a simple DNS change. As propagation occurs, any ongoing attacks are shut down immediately.

FLEXIBILITY

Reblaze works for any web platform, at any scale. It also integrates seamlessly with popular cloud services such as Amazon, Microsoft, and Google.

PRECISION

You can define separate security policies for sites, clusters of sites, subnets, IP ranges, or even for individual URLs.

RISK-FREE

Reblaze can act as an additional layer of protection to existing solutions.

COMPREHENSIVE

Reblaze is effective against all forms of Internet attack. Organizations with web assets no longer need to assemble a solution from multiple products and vendors; Reblaze does it all.

RELIABLE

The SLA includes 24/7 support and 99.999% uptime.

COMPLIANT & CERTIFIED

Reblaze's clouds are fully compliant with GDPR, SOC 1/SSAE 16/ISAE 3402, FISMA Moderate, ISO 27001, FIPS 140-2, HIPAA, and CSA. Reblaze is a PCI DSS Certified Level 1 Service Provider.