Barracuda Advanced Threat Protection

Securing Web Applications Against Malicious File Injections

White Paper

Introduction

Modern web applications have evolved into a predominant mode of data communication as well as a platform where end users can easily upload documents, images, or other files. However, the latter has led to applications accepting file uploads with any extension or type, giving attackers the opportunity to upload malicious files into applications that exploit both the organization and its clients. Therefore, filtering uploads by validating for file types or extensions is no longer an effective way of defending against such attacks.

In the recent past, in-house sandboxing techniques have been used in company networks to detect malware in files. However, deploying an appliance for sandboxing and analyzing local network files is not scalable, and it also adds severe latency and administrative overhead, which results in badly implemented security. Additionally, enhanced inspection techniques that send notifications and adequate logging are required to defend against today's file injections. By immediately notifying the administrator when an attack occurs, they have a better chance of combating threats.

Why Anti-Virus Scanning Isn't Enough

Running a business is becoming more dynamic, yet more complex. Unfortunately, this also applies to the business of malware and ransomware. Popular branches of malware (like Duqu and Miniduke) are being used to target websites, and are rarely detected by traditional anti-virus services. The origin of these infections is typically through simple actions like file uploads in web applications. Today's threats spread at a high velocity, making it difficult to detect a threat, isolate the signature, add the signature to databases, and make it publicly and continually available in a very short time. By the time the database update is available, the threat has already compromised a network's systems and has successfully covered up its tracks.

While these signature-based legacy systems are still important as a first line of defense for pre-filtering network traffic, organizations still need an additional security layer to protect against targeted malware.

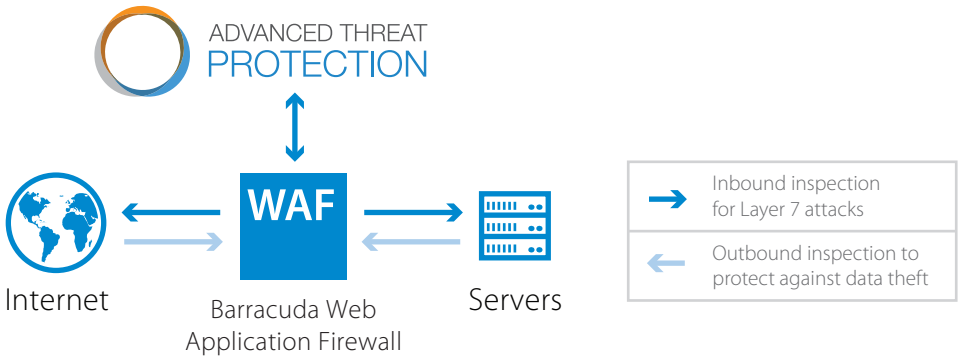
The Barracuda Difference

Today's web applications need comprehensive, reliable protection against advanced persistent threats and file injections. The Barracuda Advanced Threat Protection (BATP) is a cloud-based service used by the Barracuda Web Application Firewall to provide in-depth defense against ransomware, malware, and advanced cyber attacks. It consists of multiple layers of detection, including signature and static behavioral analysis to provide accurate detection of a variety of polymorphic attacks.

Barracuda Advanced Threat Protection is available on Barracuda's entire portfolio of security products and processes more than 20 million requests per day. This results in one of the world's most comprehensive databases of known bad IP addresses, "spyware domains," and command and control servers used by botnets.

Providing the Flexibility an Organization Needs

Administrators need to deal with more than just one file type and/or protocol. Barracuda Advanced Threat Protection gives security administrators the flexibility they need to ensure the highest quality of service possible.



Inspection

Files uploaded as multipart/form-data in POST requests is inspected by the Barracuda Advanced Threat Protection. The "Deliver and Scan" approach is used to scan the files to avoid delivery delays during the scanning process. This approach also enables incoming traffic to be inspected and processed through to the web server at faster speeds, while a copy of the file is scanned by the Barracuda Advanced Threat Protection cloud service.

The following MIME types are inspected for malware:
application/pdf
application/msword
application/vnd.ms-powerpoint
application/vnd.ms-excel
application/x-msaccess
application/vnd.openxmlformats-officedocument.presentationml.presentation
application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
application/vnd.ms-cab-compressed
application/vnd.microsoft.portable-executable
application/vnd.openxmlformats-officedocument.wordprocessingml.document
application/rtf

Detailed Logging

Upon inspection of the file, the web firewall logs are updated with information on the inspection. For example, the attack name "BATP Scan" can be used to filter the logs specific to this. The Barracuda Web Application Firewall notification service can also be used to alert the administrator of the violation so that reactive measures can be taken and malicious files can be removed.

Barracuda Advanced Threat Protection at a Glance

KEY FEATURES	THE BARRACUDA ADVANTAGE
Identify zero-day malware exploits, ransomware, targeted attacks, advanced persistent threats, and other advanced malware that routinely bypasses traditional signature-based IPS and anti-virus engines.	Easy to deploy, easy-to-use, and affordable Advanced Threat Protection (ATP).
Blocking of active content in Microsoft Office and PDF documents.	No new equipment needed.
Full interoperability with the integrated SSL Inspection: Files can be extracted and checked to detect advanced malware in the encrypted stream.	Information on identified malware is centrally stored and shared to optimize emulation.
Available for hardware and virtual appliances, as well as for Microsoft Azure and Amazon AWS.	Barracuda ATP and malware protection are available as an affordable bundle subscription.

About Barracuda Networks, Inc.

Barracuda (NYSE: CUDA) simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications, and data regardless of where they reside. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide, and are delivered in appliance, virtual appliance, cloud, and hybrid configurations. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network security and data protection. For additional information, please visit barracuda.com.

Barracuda

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com