SRC CYBER SOLUTIONS LLP

THREATX

How to Avoid the Top 3 Pitfalls of Reputation-Based WAF's

THREATS

Modern, Hybrid Cloud Environments are Increasingly Vulnerable

Due to the growing complexity of multi-cloud and internal application environments, traditional approaches to cybersecurity are no longer effective. Signature-based models are simply unable to scale and protect increasingly large attack surfaces or block the most advanced threats. This guide will help you recognize and address the common pitfalls of IP/Reputation blacklist feeds and introduce a new approach to supplement them.

Reducing the Noise, but Missing the Attack

Blacklist threat feeds are a common component in defensive toolsets as they reduce the noise that crawlers, scanners, bots and script kiddies put into your web logo by blocking IPs that have been previosly identified as malicious. Unfortunately, the growing sophistication of the threat landscape allows more advanced attackers to circumvent this approach. Most of the threat actors that appear on these lists fall into the nuisance category – trying to create WordPress accounts on your Java site, requesting non-existing CGI scripts, or running directory traversal attacks to obtain Unix passwords on a Microsoft IIS server.

As the capability of threat actors increases, the ability for traditional rule-based defenses to identify those threats decreases. Even commercial 'curated' feeds, which some vendors claim can identify sophisticated attackers, have proven pitfalls.

PITFALLS

The Top 3 Pitfalls of Blacklist Threat-Feeds

Sophisticated attackers have access to free blacklists

Blacklists are effective at identifying bots and script kiddies but are easily bypassed by sophisticated attackers. While it is unlikely that an attacker will have access to commercial blacklists, they can either search and utilize the same free lists available to a defender or assume they have been blacklisted if they can no longer access the targeted application. Either way, the attacker can discern which IP addresses are blocked and can (and will!) simply pivot to another IP address and continue with their targeted attack.

Blacklists cover only a fraction of all malicious IP addresses

Another shortcoming of blacklists is their relatively small size compared to the large number of malicious IP addresses in the wild. Some free lists contain more than 30,000 IPs. That said, we have identified botnets containing over 500,000 IP addresses, meaning a blacklist won't protect you from the hundreds of thousands of other addresses that could be targeting you. In addition, most firewalls are unable to consume a threat feed of that size.

IP/Reputation feeds, scoring and blocking are merely speed bumps

IP/Reputation feeds are not very effective against the growing number of sophisticated attacks that comprise today's threat landscape. Similarly, Geo IP reputation scoring, and TOR node blocking can stop some attackers but typically act as mere "speed bumps" for any sophisticated attacker who can proxy traffice through a compromised host anywhere in the world (including compromised servers hosted at US cloud providers).

But Wait, There's Hope

To combat the shortcomings of traditional defensive approaches and ultimately block both basic and targeted attacks regardless of where they originate, another method that goes beyond blacklists or reputation feeds is required. ThreatX has developed a Contextual Behavioral Analysis (CBA) apporach that monitors and identifies risky behavior and blocks attackers before they can do any harm.

THREATX

SRC CYBER SOLUTIONS LLP

4 STEPS

There are four steps to the ThreatX CBA approach

1. We inspect metadata from every entity that connects to a site, including the encryption type, URI, user-agent, header, cookies, POSTs, response codes, etc.

2. Once a threat is identified, we monitor and follow the attacker's path as they traverse a site.

3. Using a kill-chain based contextual approach, we build a holistic risk profile for every entity based on the techniques and behaviors they have demonstrated over time.

4. When we detect suspicious behavior, the risk level is assessed for that activity. Some activities result in a small risk increase, others in an immediate block. Equally important, legitimate users are not impacted because they do not exhibit risky behavior or because their activity never reaches a risk level that requires blocking.

This approach dramatically reduces false positives compared to a solution that makes binary blocking decisions based on static rules and signatures. ThreatX quickly identifies and blocks attackers who don't show up on reputation feeds, determines if they pivot IPs, and correlates multiple addresses into a single attacking entity.

While you should continue utilizing IP blacklists as part of your layered defense strategy, we encourage you to understand their place in the defender's toolkit. Contextual Behavioral Analysis delivers truly comprehensive and effective protection from web attacks against today's, complex, hybrid cloud environments.

Request a Free Trial

To see what a true, next-gen web application firewall solution with a managed service looks like, request your free, 15-day trial: https://www.srccybersolutions.com/contact-us

www.srccybersolutions.com | +91 120 232 0960 / 1 | sales@srccybersolutions.com

THREATX

SRC CYBER SOLUTIONS LLP