Unexpected Countries Scenario

Automated Attacks from Unexpected Countries is a form of web application intrusion using botnets to exploit holes in your web applications. In this white paper, we briefly discuss the Automated Attacks from Unexpected Countries scenario, provide an example of how it is used, explain how NetGladiator stops the attack, and tie this in to your overall layered security approach.

Automated Attacks from Unexpected Countries Description

From almost the moment a web server has a public facing IP address, botnets from all over the world are automatically scanning it for vulnerabilities. Often, these attacks originate from countries that house very few potential users or customers for your business. Botnets can be used maliciously to perform Denial of Service (DoS) attacks, website scraping, automated downloads, etcetera.

Example

You are a local business based in the United States. You sell videos to schools that teach kids how to do math. You have some online interfaces and also sell the videos online. Because the Internet is a global entity, your website is being hacked at by robots originating in China, Iran, and Morocco every day. While possible, it is very unlikely that a legitimate request for your website is coming from someone in these locations.

You are putting your data at grave risk by allowing connections from IP spaces coming from unexpected countries (e.g. countries outside your normal scope of business) for the possibility of a small sale.

How NetGladiator Stops This Attack

In this case, it is best to not even allow connections from unexpected countries (countries outside your normal scope of business). This may sound harsh and somewhat sweeping at first, but good security is all about risk vs. cost. Sure, this might turn away a few potential clients, but it will keep you less visible to a large, malicious botnet. NetGladiator is capable of blocking IP ranges right off the bat. IP addresses can be geo-located with relative accuracy, and NetGladiator allows you to black list these IP addresses.

The NetGladiator is a key device in a layered security approach. Its behavior-based anomaly detection identifies potential attackers through recognizing unusual patterns of behavior, as hackers explore and utilize your website much differently than a normal user.

Layer This With...

Diligent log review is the key to discovering locations of attacks hitting your websites. If you notice patterns in the logs indicating attacks from a specific IP range, block this IP set in NetGladiator's user interface.

When developing an IT security policy and implementing security controls, the single most important thing to consider is how the different controls you use will layer within your security profile. Because no single piece of equipment or software will be able to thwart 100% of attacks, good layering provides the best chance to stop a hacker from their ultimate goal.

To Learn More...

We would be a happy to discuss the NetGladiator technology, to help you to determine if this is the right solution for you. Please email ips@apconnections.net or call us at **303.997.1300 x123**.

About APconnections, Inc.

APconnections is an innovation-driven technology company that delivers best-in-class network traffic management solutions to give our customers better networks, with zero maintenance, at the best prices. We specialize in turn-key bandwidth shaping and intrusion prevention system (IPS) appliances.

Since 2003, APconnections' mission has been to provide simple turn-key network optimization appliances to any network topology. Our products are simple to install, easy to use, require little maintenance, and are offered at the best prices.

APconnections is based in Lafayette, Colorado, USA. We released our first commercial offering in July 2003, and since then thousands of customers all over the world have put our products into service. Today, our flexible and scalable solutions can be found in many types of public and private organizations of all sizes across the globe, including: Fortune 500 companies, major universities, K-12 schools, Internet providers, law firms, hotels, hospitals, libraries, business centers, small businesses, non-profits, military, and government agencies on six (6) continents.