ATLAS Intelligence Feed

For Arbor Sightline and Threat Mitigation System

HIGHLIGHTS

- **Dynamic Updates for Accurate Protection** – Updates with the latest threat information to maintain the most accurate detection policies.
- **Campaign-Based Attack Identification** – Identifies singular points of compromise and related attacks that are part of an orchestrated campaign.
- **Fast Attack Response** – Provide valuable context to each attack, enabling a faster, more informed response.
- **Threat Validity & Prioritization** – Goes beyond collecting and analyzing threat data to validate that threats are real and current.

Combine the sheer amount of Internet traffic your organization consumes with the number of security threats possible, you begin to see the risks your company faces. Threat intelligence must be a part of your protection strategy. Having actionable intelligence could mean the difference between prepared and protected, versus unaware and unguarded. Effective security intelligence, not only identifies attacks, but understands and catalogs the attack infrastructure, methods and other indicators so that broader, more proactive measures can be taken with confidence.

Dynamics of an Effective Threat Intelligence Feed

Effective threat intelligence requires three things:

1. A continuous source of real world network traffic and data;
2. A robust infrastructure for gathering and analyzing network traffic and threat data; and
3. A dedicated team to manage data and add the “human intelligence” to the analysis.

Truly great threat intelligence goes beyond collecting and analyzing attack data. It should make a marked improvement over existing staff and processes. This information must be actionable and seamlessly integrated into your security posture. The risk from each threat should be clear, and the actions taken should be evident.

The ATLAS® Intelligence Feed, from Arbor enables you to quickly address multi-vector attacks, whether they be DDoS-related, or part of a larger advanced threat.

Applying ATLAS Intelligence

ATLAS Intelligence Feed for Arbor Sightline and Arbor Threat Mitigation System provides you with detailed information about DDoS attacks, and the ability to quickly detect them before they cause internal outages. Examples of the policies and countermeasures in the ATLAS intelligence Feed are included below:

Early Warning System

The difference between being ready for an attack versus reacting to an attack that is already in progress can represent long-term outage, and revenue loss. With the ATLAS Intelligence Feed, you also have access to an early warning service which provides targeted early warnings about potential DDoS attacks as identified from the ATLAS botnet infrastructure.

	Threat Policy Types	SP	TMS+
Command & Control	• Peer to Peer • HTTP • IRC	✓	
DDoS Reputation Threats	• Attacker • Target	✓	
Malware	• Webshell • Ransomware • RAT • Fake Anti Virus • Banking • Virtual Currency • Spyware • Drive By • Social Network • DDoS Bot • Dropper • Ad Fraud • Worm • Credential Theft • Backdoor • Exploit Kit • Point of Sale • Other	✓	
IP Geo Location	• Identification by country for sources of inbound traffic • Identification by country for destinations of outbound traffic	✓	✓
DDoS RegEx	• Identifies DDoS attackers based upon IP address indicators from ATLAS • Identifies DDoS targets based on indicators from ATLAS HTTP Flooder		✓

Figure 1: Example threats identified using the AIF Standard feed. All countermeasures and policies are continuously updated, so above list may change at any time.

As new attack information is discovered, the ATLAS Intelligence Feed is updated, and changes are delivered automatically to your Arbor Sightline and Arbor Threat Mitigation System via a subscription service over a secured SSL connection arming them with the latest threat intelligence. The best way to be protected, is to have the most up-to-date intelligence from the broadest view, enriched by seasoned experts.

The world-class team of security researchers are dedicated to discovering and analyzing emerging internet threats and developing targeted defenses. Arbor employs a sophisticated combination of attack data collection, partner information and analysis tools to create policies that detect threats while providing context so that you can make informed protection and mitigation decisions. This is the ATLAS Intelligence Feed.

HOW DOES THIS FEED DETECT THREATS TO MY NETWORK?

- Identifies threats regardless of attack volume; no waiting for an attack to reach a volume threshold before defending.
- Uses multiple levels of protection aligning with confidence levels.
- Applies attack intelligence contributed from advanced controlled detonation of millions of malware samples.
- Includes reverse engineering of specific malware, and all malware related to a botnet.
- Actively monitoring Internet threats around the clock utilizing Arbor's global Sensors network.
- Historical tracking of botnets, their location and attack methods over time.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us