ARBOR NETWORKS
The Security Division of NETSCOUT

DON'T WASTE TIME ON NOISE: ACTIVE THREAT VISIBILITY AT A GLOBAL SCALE

Defeating Attack Campaigns with Arbor Networks' Threat Indicator Policies

About Arbor Networks

Arbor Networks, the cyber security division of NETSCOUT, helps secure the world's largest enterprise and service provider networks from DDoS attacks and advanced threats. Arbor is the world's leading provider of DDoS protection in the enterprise, carrier and mobile market segments, according to Infonetics Research. Arbor's advanced threat solutions deliver complete network visibility through a combination of packet capture and NetFlow technology, enabling the rapid detection and mitigation of malware and malicious insiders. Arbor also delivers market-leading analytics for dynamic incident response, historical analysis, visualization and forensics. Arbor strives to be a "force multiplier," making network and security teams the experts. Our goal is to provide a richer picture into networks and more security context so customers can solve problems faster and reduce the risks to their business.

To learn more about Arbor products and services, please visit our website at arbornetworks.com.

OVERVIEW

Sometimes the most dangerous threats to today's business network are those hardest to detect. With Arbor Network's ATLAS Intelligence Feed (AIF) threat indicator policies you can detect and defeat today's advanced attack campaigns.

Campaigns Are More Than Malware

Attack campaigns involve detailed planning: not only who to target, but the best infrastructure to use, how to monetize the attack, and trying different strategies until they are successful. Attackers seek to reuse tactics, techniques and procedures (TTPs) – more than just malware – and automate the attack as much as possible. And often victims are not even aware of an attack until the damage has been done.

A finance director in a global enterprise opens an email attachment from what seems to be a legitimate source. Unfortunately, the director has inadvertently — and unknowingly — downloaded PlugX, a remote access tool (RAT) being used as part of an advanced attack campaign. PlugX has been used as part of attack campaigns since at least 2008. It enables a remote bad actor to execute commands on infected machines to gather network information, log keystrokes, take screenshots, look into memory, etc.

In this case, PlugX follows remote Command & Control (C2) instructions to capture the director's keystrokes and send the data back to bad actors to exploit further. From this data the attackers compromise the director's login and password to access the organization's ERP finance module. The attackers now appear as a legitimate user, and can access financial records that give them valuable corporate information, to be held for ransom, sold, or used to do additional damage to the enterprise.

One of the most worrisome aspects of a successful advanced attack is that many initial penetrations cannot be detected by endpoint antivirus solutions that identify only isolated signatures. And once a network is compromised there may be no performance problems or clear alerts to signal the seriousness of the infiltration. In most cases the enterprise is not even aware they have been compromised until alerted by law enforcement or a third party — usually after the damage has been done.

How do you protect yourself against this kind of attack?

Intelligence to Detect and Defeat an Advanced Attack Campaign

Arbor Network's AIF threat indicator policies provide you knowledge without the noise. Attack campaigns include tactics, techniques and procedures (TTPs) that comprise an orchestrated, ongoing set of operations against well-researched targets. Advanced campaigns require command and control (C2) communications. The detection and mitigation of attack campaigns requires visibility into your entire network traffic—you can't catch what you can't see. But at the same time you cannot investigate everything; there simply is too much data.

The challenge becomes recognizing and prioritizing the truly dangerous Indicators of Compromise (IoC). You'd like to know, with a **high level of confidence**, what events are serious. And you need this information in real time so you can prioritize and use your resources most effectively.

Defending against campaigns requires a **more complete, connected picture of what you are up against**. What is the likely goal of this campaign, what other components or techniques might it employ—and where is it likely to go to next? For example, security professionals armed with C2 domains connected to specific, active threat indicators are better prepared to track the full extent of compromise faster and with a greater degree of confidence.

For the scenario above, your security team could be more effective and efficient if they knew the PlugX malware used against the finance director likely re-purposed the C2 domains involved in a previous EvilGrab watering hole attack. And these same domains had been associated with other, recent campaigns where perpetrators leveraged compromised legitimate credentials to compromise authentication servers to lay the groundwork for future attacks.

Such actionable threat intelligence is hard to come by. Most organizations don't have the visibility at Internet scale, the resources, nor the expertise to provide high-fidelity, campaign level threat indicator intelligence.

Defending against campaigns requires a more complete, connected picture of what you are up against.

Figure 1 *Depiction of an Attack Campaign*

ATLAS® Intelligence Feed (AIF) from Arbor Networks

Arbor Network's AIF is a service of the Arbor Network's Security Engineering and Response Team (ASERT).

For over a decade ASERT's world-class security analysts have been building the tools and front-line database to analyze malware at Internet scale. As threat information is captured and analyzed by ASERT, the AIF is updated with **threat indicator policies**. Threat indicator policies are high-fidelity, actionable intelligence that identify known bad traffic components with a high degree of confidence (see chart).

ASERT ingests data from one of the world's largest collection of darknet sensors, honey pots and sinkholes, including Arbor's Active Threat Level Analysis System (ATLAS). The ASERT team scrutinizes the data using custom tools and techniques developed by security analysts for analysts. This involves more than sandboxing, reverse engineering or deconstruction of botnet behavior. One example: ASERT has built unique custom analyzers to track malware families and correlate them with specific IoC and known attack campaigns.

The AIF is delivered over a secured SSL connection to all Arbor Network's products. Your team is automatically armed with indicator policies containing the latest threat intelligence, helping you detect all the attack components, track their behavior and thwart attack campaigns in their entirety working within your network.

Policies in Arbor AIF **Standard Subscriptions**

THREAT POLICY TYPES		
Command & Control (C2)	• Peer to Peer • HTTP	
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
IP Geo Location	• Identification by country for sources of inbound traffic • Identification by country for destinations of outbound traffic	
ET Pro	• IDS Signatures (Spectrum helps tune these alerts to most critical assets)	

Policies in Arbor AIF **Advanced Subscriptions**

THREAT POLICY TYPES		
Location-Based Threats	• Traffic Anonymization Services • TOR • Proxies	• Sinkholes • Scanners • Other
Email Threats	• Spam • Phishing	
Targeted Attacks	• APT • Hactivism • RAT	• Watering Hole • Rootkits

About ATLAS®

Arbor's Active Threat Level Analysis System (ATLAS) sees more internet traffic, and collects more data on that traffic, than any service. ATLAS monitors over one-third of all internet traffic providing near-real-time visibility into today's' threats, fueling Arbor's mission to help keep the internet stable and secure.

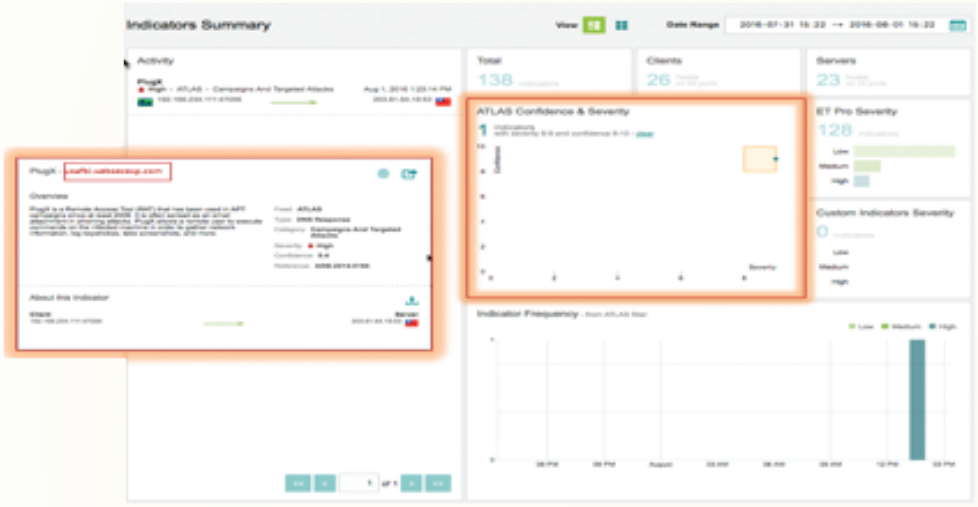

Figure 2 *Screenshots of PlugX Campaign — AIF Policy Detected in Spectrum Console*

How AIF Policies Help You Detect and Defeat Advanced Attack Campaigns

Threat indicator policies within Arbor Network's Spectrum helps your team quickly identify, with a high degree of confidence, IoCs associated with the most dangerous threats. You are also armed with intelligence of the attack's TTPs to quickly track how/where it is likely to spread in your network. Spectrum provides real-time visibility into network conversations between hosts and connection points of interests. The UI is organized around prioritized IoC and response workflows, automatically correlated with underlying policy intelligence. The user can interactively navigate, search and pivot through **both threat indicator and traffic data,** giving them the total visibility they need to thoroughly discover, investigate and respond to attacks.

For the scenario described above, threat indicator policy intelligence automatically identifies C2 communications between the finance director's host and bad actors. The indicator page shows severity and confidence levels are high: a DNS communication to an external server, 'usafbi.websecexp.com', is a known C2 domain recently used by PlugX malware. The operator can move quickly to remove that host from the network, or maintain for further observation.

The operator also knows from the broader policy intelligence that this campaign likely attempted to compromise the authentication server. Using the Spectrum investigations module the operator can quickly look back over weeks, even months of network traffic to focus on the authentication server profile and specific network connections in a single view. This rapid, focused visualization of potential bad traffic does not reveal any further compromise; it looks like they isolated the PlugX compromise in time.

The AIF threat indicator policies with specific and broader attack campaign intelligence allow you to quickly evaluate the full range of TTPs within a currently active attack. With greater visibility on and understanding of what might be happening within your network you can more rapidly prioritize where you spend your resources. Campaign intelligence enables you to eliminate more noise and become more efficient — and effective — at protecting your network.

See Threat Indicator Policies in Action

Real-time traffic visibility, past and present, and informed workflows can further enhance your security posture. Armed with the context to prioritize and correlate seemingly disparate events, security professionals can seek out, track and defeat attacks *hidden in their infrastructure.* You can become proactive, go on the hunt: where are we compromised, who was compromised, and what has happened in the network to threaten our assets and operations.

Find more information by reading the ATLAS Intelligence Feed Data Sheet at arbor.link/attack

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales
Toll Free +1 855 773 9200

Europe
T +44 207 127 8147

Asia Pacific
T +65 6664 3140

Latin & Central America
T +52 55 4624 4842

www.arbornetworks.com

ARBOR® NETWORKS

The Security Division of NETSCOUT

UC/AIF/EN/0717-LETTER