Data Sheet

ATLAS® INTELLIGENCE FEED

Uma resposta mais inteligente a ameaças à segurança e disponibilidade.

Dado o influxo de ameaças que atacam sua empresa de todos os ângulos, pontos de entrada e vetores possíveis, o que realmente é necessário para se manter à frente dos invasores? Contexto. Esse contexto pode ajudar você a avaliar os riscos, priorizar o tempo da sua equipe de operações de segurança e enfrentar a próxima (entre muitas) ameaça. A inteligência de segurança correta alimenta a criação de mecanismos para reconhecer e bloquear os ataques baseados em rede, algumas vezes. No entanto, a inteligência de segurança efetiva não apenas identifica os ataques, mas entende e cataloga a infraestrutura, os métodos e outros indicadores do ataque para que medidas mais amplas e proativas possam ser tomadas com confiança.

Como lidar com ameaças avançadas

O ATLAS Intelligence Feed, ou AIF, da Arbor Networks equipa os clientes com políticas e medidas defensivas que lhes permitem lidar rapidamente com ataques como parte de uma ameaça avançada ou ataque DDoS. O AIF é um serviço da Arbor Security Engineering and Response Team (ASERT) e permite que os clientes se beneficiem diretamente da visão detalhada e ampla dos recursos de pesquisa da Arbor.

A Arbor Networks tem um potente portfólio de produtos projetado para as redes corporativas e de provedores de serviços, todas as quais se beneficiam do consumo do AIF. À medida que novas informações sobre ataques são descobertas, o AIF é atualizado e as alterações são fornecidas automaticamente para os produtos da Arbor por meio de uma assinatura por conexão SSL segura, equipando-os com a inteligência contra ameaças mais recentes para impedir os ataques DDoS ou ameaças avançadas dos dias de hoje. A melhor maneira de proteger sua organização é ter a inteligência mais atualizada da mais ampla visão, enriquecida por especialistas experientes. Este é o ATLAS Intelligence Feed.

Dinâmica de um feed de inteligência contra ameaças eficaz

A inteligência contra ameaças eficaz exige três coisas:

- Uma fonte contínua de dados sobre tráfego de rede e ameaças do mundo real;
- Uma infraestrutura robusta para obtenção e análise de dados sobre tráfego de rede e ameaças;
- E uma equipe dedicada para gerenciar tudo acima e adicionar um aspecto de "inteligência humana" à análise.

No entanto, uma inteligência contra ameaças verdadeiramente excelente vai além de simplesmente coletar e analisar dados do ataque. Ela deve promover melhorias significativas nos processos e nas equipes existentes por meio da integração perfeita com seu programa de segurança, o que significa que as informações devem ser acionáveis. O risco de cada ameaça deve estar claro e as ações a serem tomadas devem estar evidentes.

Principais recursos e benefícios

Atualizações dinâmicas para proteção precisa
O AIF é atualizado com as informações sobre ameaças mais recentes para manter as mais precisas políticas de detecção em todos os produtos da Arbor Networks.

Identificação de ataques baseados em campanha
Ao combinar dados do ataque de diversas fontes e focar nas características do malware, o AIF identifica não apenas pontos singulares de comprometimento, mas ataques relacionados como parte de uma campanha.

Resposta rápida ao ataque
As políticas do AIF fornecem contexto valioso para cada ataque, permitindo uma resposta mais fundamentada e rápida.

Priorização e validade do ataque
Além de coletar e analisar dados sobre ameaças, a ASERT vai um passo além para validar que as ameaças sejam reais e atuais.

ARBOR® NETWORKS
The Security Division of NETSCOUT

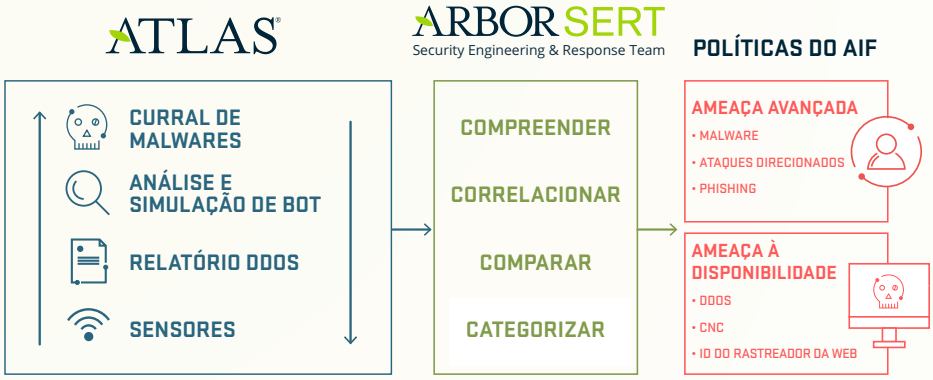

Figura 1 *O ATLAS usa uma variedade de ferramentas e processos para coletar e analisar dados de ameaças. A equipe se concentra nos recursos e no potencial dos ataques, extraindo diversos indicadores da campanha de um ataque. Esses indicadores são entregues aos produtos da Arbor por meio do ATLAS Intelligence Feed.*

A equipe de pesquisadores da área de segurança de classe mundial da Arbor está dedicada a descobrir e analisar ameaças emergentes na Internet e a desenvolver defesas direcionadas. A Arbor utiliza uma combinação sofisticada de coleta de dados do ataque, informações de parceiros e ferramentas de análise para criar políticas do AIF que não somente detectam ameaças, mas também fornecem o contexto necessário para decisões fundamentadas sobre mitigação.

Uma das principais tecnologias por detrás do AIF é a inteligência de reputação dinâmica da Arbor. A inteligência de reputação dá validade aos indicadores de ameaça que constituem as políticas do AIF. À medida que a ASERT coleta informações sobre tráfego e ameaças, ela pode juntar vários elementos da ameaça, incluindo de quais outros tipos de comprometimento um malware específico pode ser capaz. Entretanto, para evitar tomar medidas contra uma ameaça que ainda não se materializou, a inteligência de reputação fornece prova clara e demonstrável de quando e por quanto tempo um determinado IP, DNS ou URL foi comprometido. A validação de ataques é acrescentada a políticas do AIF relevantes por meio de pontuação de confiança. Esse tipo de validação de ataques é fornecido a cada política do AIF entregue aos produtos da Arbor na forma de pontuação de confiança, de modo que os usuários possam estar certos de que uma ameaça identificada pelo produto seja significativa e real.

Aplicação do ATLAS Intelligence

Cada produto do portfólio da Arbor Networks foi projetado para consumir o AIF, embora todos eles usem diferentes partes do feed para informar diferentes ações nos produtos. Alguns produtos analisam o NetFlow e outros investigam pacotes de rede. As políticas do AIF incluirão informações pertinentes a cada produto.

Arbor Networks® APS

Além de bloquear as ameaças à disponibilidade baseadas em limites de largura de banda, o APS usa as políticas do AIF para identificar vários tipos de ataques DDoS, incluindo ataques "baixos e lentos" que visam a camada de aplicativo. Além disso, o AIF ajuda o APS a detectar e impedir certas categorias de botnets de comprometer a rede. Ao impedir essas ameaças à disponibilidade e de botnets de entrarem na rede, ele permite que outros dispositivos de segurança façam os trabalhos a que foram destinados.

Arbor Networks® Spectrum

A inteligência de segurança do ATLAS no Spectrum permite que as organizações pesquisem mais a fundo os eventos de ataques para análise forense. Os indicadores de ataques presentes no AIF ajudam a identificar do que o ataque é/foi capaz na rede e por onde se espalhou. Além disso, as organizações podem sobrepor essas informações sobre ameaças com tráfego entrando e saindo dos ativos mais críticos, com o contexto e as informações para escalar eventos para investigação adicional.

—

Como o AIF protege as organizações contra DDoS e botnets?

O AIF provou ser eficaz por muitos clientes da Arbor Networks no bloqueio dos ataques sofisticados, complexos e destinados mais recentes.

Para detectar de forma mais precisa as ameaças à rede, o AIF:

- Identifica ameaças independentemente do volume do ataque; sem esperar que um ataque atinja um limite de volume antes de se defender.
- Usa vários níveis de proteção alinhando-se aos níveis de confiança.
- Aplica inteligência de ataque originada da detonação controlada avançada de milhões de exemplos de malware.
- Inclui engenharia reversa de malwares específicos, além de todos os malwares relacionados a um botnet.
- Monitora de forma ativa as ameaças na Internet durante todo o tempo utilizando a rede de sensores globais da Arbor.
- Controla o histórico de botnets, seus locais e métodos de ataque ao longo do tempo.
- O ATLAS é um projeto colaborativo com mais de 300 clientes que concordaram em compartilhar dados de tráfego de forma anônima totalizando aproximadamente um terço de todo o tráfego de Internet.

Arbor Networks® SP

A inteligência de segurança do AIF fornece aos clientes do SP a capacidade de detectar rapidamente uma grande escala de ataques DDoS antes que eles causem interrupção dos serviços internamente ou nos clientes.

Arbor Networks® TMS

As políticas do AIF no TMS dão às organizações informações detalhadas sobre os ataques DDoS para que, com rapidez e confiança, comecem a bloqueá-los. Esta precisão é crítica no bloqueio de ataques maliciosos que podem resultar em tempos de inatividade onerosos. O AIF fornece esse mesmo nível de proteção ao produto de proteção contra vDDoS do Cisco ASR 9000.

Decomposição do Intelligence Feed

Há duas assinaturas disponíveis no AIF: Padrão e Avançada. Com duas assinaturas, os clientes podem escolher o nível de detecção e/ou proteção contra ataques que se adeque às necessidades deles.

AIF Padrão

Com o feed padrão, os clientes podem detectar e/ou resolver alguns dos mais predominantes ataques que atingem as empresas atualmente, incluindo malware, botnets e ataques DDoS. As políticas e medidas preventivas são atualizadas com novas informações sobre ataques para proporcionar detecção ampla e precisa. Exemplos das políticas e medidas preventivas incluídas nesse feed são mostradas abaixo.

	Tipos de políticas de ameaças		APS	Spectrum	SP	TMS+
Comando e controle	• Ponto a ponto • HTTP • IRC		✔	✔	✔	
Ameaças de reputação de DDoS	• Invasor • Destino		✔	✔	✔	
Malware	• Webshell • Ransomware • RAT • Antivírus falso • Bancos • Moeda virtual • Spyware • Drive By • Rede social	• DDoS Bot • Dropper • Fraude de anúncio • Worm • Roubo de credencial • Backdoor • Kit de exploração • Ponto de venda • Outros	✔	✔	✔	
Localização geográfica de IP	• Identificação por país para origens de tráfego de entrada • Identificação por país para destinos de tráfego de saída		✔	✔	✔*	✔*
DDoS RegEx	• Identifica invasores DDoS baseado em indicadores de endereço IP do ATLAS • Identifica destinos DDoS baseado em indicadores do HTTP Flooder do ATLAS		✔			✔
Identificação do rastreador da Web	Identificação de conexões de entrada com os serviços da Web de mecanismos de pesquisa conhecidos		✔			
ET Pro	Assinaturas de IDS			✔		

Figura 2 *Exemplo de ameaças identificadas com o uso do AIF Padrão. Todas as medidas preventivas e políticas são continuamente atualizadas, portanto, a lista acima pode mudar a qualquer momento.*

Como a Arbor Networks está posicionada de forma exclusiva para lidar com ameaças avançadas

A Arbor tem uma história em pesquisa de botnet e mitigação de DDoS.

Como o DDoS evoluiu de uma simples tática de diversificação para um recurso de malware e botnets usados em crimes cibernéticos e ataques de APT, a Arbor expandiu sua equipe ASERT e seus recursos de pesquisa para identificar e analisar tipos adicionais de ameaças. A abordagem da ASERT à inteligência contra ameaças agora inclui diversos fatores que não apenas ajudam a identificar ameaças, mas também confirmar sua penetração e gravidade. Estão incluídos:

- Monitoramento de reputação e controle ativo de campanhas de ataques baseados em indicadores do mundo real da Red Sky Alliance.
- Um sistema de backend avançado para análise de malware composto de tecnologia de parceiro externo juntamente com processos e análises desenvolvidos internamente.

A ASERT usa esses dados e análise de ameaças para desenvolver o AIF, que é usado por clientes da Arbor para detectar eventos que ocorrem na rede ou em torno dela. A combinação desta microvisão (na rede) com a macrovisão do tráfego de Internet (entregue pelo portal do ATLAS) dá aos clientes uma vantagem distinta para lidar com ameaças avançadas.

* *Localização geográfica de IP atualizada no SP, TMS e produtos de proteção contra DDoS do Cisco ASR 9000 por meio de patch do produto.*

* *As políticas do AIF usadas no TMS são as mesmas da proteção contra DDoS do Cisco ASR 9000.*

AIF Avançado

O AIF Avançado foi projetado para as organizações preocupadas com ataques dissimulados e mais sutis. Com uma assinatura desse feed, os clientes recebem todas as medidas preventivas e políticas incluídas no feed Avançado, além de políticas adicionais para descobrir comportamentos de ataques indicativos de ataques contínuos, no estilo de campanha, aqueles que são altamente personalizados para um negócio específico e que são difíceis de detectar porque podem parecer legítimos. Exemplos de medidas preventivas e políticas incluídas nessa assinatura são mostrados abaixo.

	Tipos de políticas de ameaças	APS	Spectrum	SP	TMS
Ameaças baseadas em localização	• Serviços de anonimato de tráfego • TOR • Proxies • Sinkholes • Scanners • Outros	✔	✔		
Ameaças de e-mail	• Spam • Phishing	✔	✔		
Ataques direcionados	• APT • Hacktivismo • RAT • Watering Hole • Rootkits	✔	✔		
Dispositivos móveis	• Mobile C&C • Spyware • Aplicativos maliciosos	✔	✔		

Figura 3 *Exemplo de ameaças identificadas com o uso do feed do AIF. Medidas preventivas e políticas são continuamente atualizadas, portanto, a lista acima pode mudar a qualquer momento. As políticas da assinatura Avançada não estão atualmente disponíveis para clientes de proteção contra DDoS do SP, TMS ou Cisco ASR 9000.*

ARBOR NETWORKS
The Security Division of NETSCOUT

Estados Unidos
T: +1.781.362.4300
contact@arbor.net

Brasil
T: +55.11.4380.8035
brasil@arbor.net

México, Caribe & Central America
T: +52.55.4624.4842
mxcca@arbor.net

North of Latin America
T: +571.508.7099
nola@arbor.net

South of Latin America
T: +54.11.5218.4007
sola@arbor.net

www.arbornetworks.com

DS/AIF/PT/0717-LETTER