Hoja de datos

ATLAS® INTELLIGENCE FEED

Una respuesta más inteligente a las amenazas a la disponibilidad y la seguridad.

Dada la afluencia de amenazas que llegan a su empresa desde cualquier ángulo, punto de entrada y vector posible, ¿qué es lo que realmente necesita para adelantarse a los atacantes? Contexto. El contexto puede ayudarlo a medir el riesgo, priorizar el tiempo de su equipo de operaciones de seguridad y pasar a la próxima amenaza (entre varias) que esté al alcance de la mano. La correcta inteligencia de seguridad alimenta la creación de mecanismos para reconocer y bloquear los ataques basados en la red, parte del tiempo. Sin embargo, una inteligencia de seguridad efectiva no solamente identifica ataques, sino que también comprende y cataloga la infraestructura, los métodos y otros indicadores del ataque, de modo tal que puedan tomarse medidas más amplias y proactivas con confianza.

Tratar las amenazas avanzadas

ATLAS Intelligence Feed, o AIF, de Arbor Networks, equipa a los clientes con políticas y tácticas defensivas que les permiten abordar ataques rápidamente como parte de una amenaza avanzada o ataque DDoS. La AIF es un servicio del Arbor Security Engineering and Response Team (ASERT) y permite a los clientes beneficiarse directamente de la amplia y profunda capacidad del equipo de investigación de Arbor.

Arbor Networks cuenta con una fuerte cartera de productos diseñados tanto para la empresa como para las redes de proveedores de servicios; y todos se benefician del consumo de la AIF. En cuanto se descubre nueva información sobre ataques, la AIF se actualiza y los cambios llegan a los productos de Arbor automáticamente por medio de una suscripción hecha a través de una conexión SSL segura, lo que los equipa con la inteligencia de amenazas más reciente para frustrar los ataques DDoS o las amenazas avanzadas de los tiempos modernos. La mejor manera de proteger a su organización es tener la inteligencia más actualizada desde la visión más amplia, enriquecida por veteranos expertos. Y esto es ATLAS Intelligence Feed.

La dinámica de una fuente de inteligencia de amenazas efectiva

Una inteligencia de amenazas efectiva requiere tres cosas:

- Una source continua de datos sobre el tráfico de red y las amenazas del mundo real;
- Una infraestructura robusta que recopile y analice datos sobre el tráfico de red y las amenazas;
- Y un equipo dedicado que administre todo lo que anterior y que le agregue un toque de "inteligencia humana" al análisis.

Sin embargo, la verdadera inteligencia de amenazas va más allá del simple hecho de recopilar y analizar datos de ataques. Debe lograr una mejora marcada sobre el personal y los procesos existentes a través de una perfecta integración en su programa de seguridad, lo que a su vez significa que la información debe ser procesable. El riesgo de cada amenaza debe ser claro, y las acciones que hay que realizar deben ser evidentes.

—

Características y beneficios principales

Actualizaciones dinámicas para una protección precisa
La AIF se actualiza con la información de amenazas más reciente para mantener las políticas de detección más precisas en todos los productos de Arbor Networks.

Identificación de ataques basados en campañas
Al combinar datos de ataques de varias sources y enfocarse en las características del malware, la AIF identifica no solo puntos únicos de peligro, sino ataques relacionados como parte de una campaña.

Respuesta rápida a los ataques
Las políticas de la AIF brindan un contexto de valor para cada ataque, lo que permite una respuesta más rápida y más informada.

Validez y prioridad de las amenazas
Además de recopilar y analizar datos de amenazas, ASERT da un paso más allá para validar que las amenazas sean tanto reales como actuales.

ARBOR® NETWORKS
The Security Division of NETSCOUT

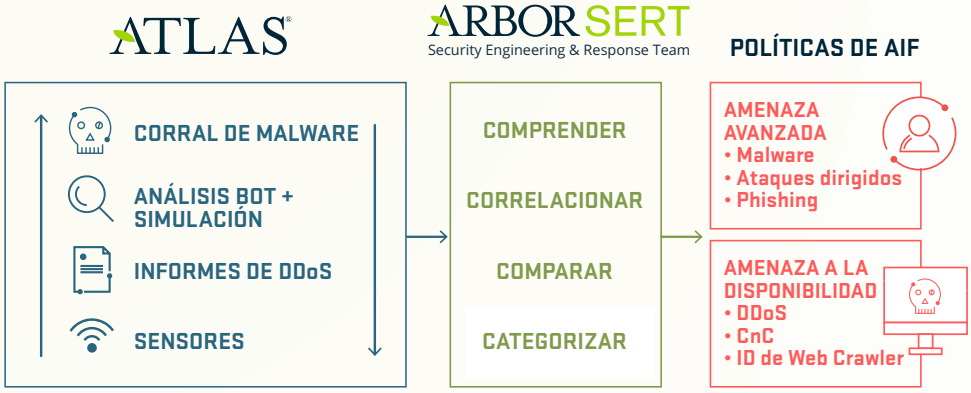

Figura 1 *ATLAS usa varias herramientas y procesos para recopilar y analizar datos de amenazas. El equipo se enfoca en las capacidades y el potencial de los ataques, y extrae varios indicadores de una campaña de ataques. Dichos indicadores se envían a los productos Arbor por medio de ATLAS Intelligence Feed.*

El equipo de clase mundial de investigadores sobre seguridad de Arbor está dedicado a descubrir y analizar amenazas de Internet emergentes, y a desarrollar defensas dedicadas. Arbor utiliza una sofisticada combinación de recopilación de datos de ataques, información sobre socios y herramientas de análisis para crear políticas de AIF que no solo detectan amenazas sino que también proveen el contexto requerido para tomar decisiones de mitigación informadas.

Una de las tecnologías claves que subyace en la AIF es la inteligencia de reputación dinámica de Arbor. La inteligencia de reputación da validez a los indicadores de amenazas que conforman las políticas de la AIF. A medida que ASERT recopila información sobre tráfico y amenazas, puede descifrar varios elementos de la amenaza, lo cual incluye qué otros tipos de peligros podría implicar un malware específico. Pero a fin de evitar tomar acciones sobre una amenaza que no se materializó hasta el momento, la inteligencia de reputación proporciona pruebas claras y demostrables de cuándo y por cuánto tiempo un IP, DNS o URL específico ha estado en peligro. Se agrega la validación de ataques a políticas relevantes de la AIF a través de puntajes de confianza. Este tipo de validación de ataques se provee en cada política de AIF que se entrega a los productos de Arbor bajo la forma de un puntaje de confianza, para que los usuarios puedan estar seguros de que una amenaza identificada por el producto es importante y real.

Aplicar la inteligencia de ATLAS

Cada producto de la cartera de Arbor Networks está diseñado para consumir la AIF, aunque todos utilicen partes diferentes de la fuente para informar acciones diferentes que ocurren entre los productos. Algunos de los productos analizan Netflow, y algunos otros productos examinan los paquetes de la red. Dentro de la AIF, las políticas incluyen información relevante para cada producto.

Arbor Networks® APS

Más allá de bloquear las amenazas a la disponibilidad basado en los umbrales de ancho de banda, el APS usa las políticas de la AIF para identificar varios tipos de ataques DDoS, incluidos ataques "bajos y lentos" dirigidos a la capa de aplicaciones. Además, la AIF ayuda a que el APS detecte y detenga ciertas categorías de botnets para que no pongan en peligro la red. Al impedir que estas disponibilidades y amenazas de botnet ingresen en la red, permite que otros dispositivos de seguridad realicen el trabajo para el cual fueron diseñados.

Arbor Networks® Spectrum

La inteligencia de seguridad ATLAS incluida en Spectrum permite que las organizaciones exploren profundamente los eventos de ataques para realizar análisis forenses. Los indicadores de ataques presentes en la AIF identifican de qué es o era capaz el ataque en la red, y adónde se dispersó. Además las organizaciones pueden superponer esta información de amenazas con el tráfico que va y viene desde los activos más fundamentales, con el contexto y la información para escalar eventos a fin de investigar con mayor detalle.

—

¿Cómo protege la AIF a las organizaciones contra DDoS y botnets?

La AIF ha probado ser eficaz para muchos clientes de Arbor Networks en cuanto al bloqueo de los ataques dirigidos más recientes y más complejos y sofisticados.

Para detectar amenazas a la red con mayor precisión, la AIF:

- Identifica amenazas en forma independiente del volumen del ataque; no espera a que un ataque alcance un umbral de volumen para defenderse.
- Usa varios niveles de protección alineados con niveles de confianza.
- Aplica inteligencia de ataques que proviene de la detonación controlada y avanzada de millones de muestras de malware.
- Incluye ingeniería inversa de malware específico, así como de todo el malware relacionado con un botnet.
- Supervisa activamente las amenazas de Internet todo el tiempo por medio del uso de la red global de sensores de Arbor.
- Hace un rastreo histórico de los botnets, sus ubicaciones y métodos de ataque a lo largo del tiempo.
- ATLAS es un proyecto de colaboración con más de 300 clientes que acordaron compartir datos de tráfico anónimos con Arbor, lo que es aproximadamente un tercio de la totalidad del tráfico de Internet.

Arbor Networks® SP

La inteligencia de seguridad de la AIF les brinda a los clientes de SP la capacidad de detectar rápidamente ataques DDoS en gran escala antes de que causen un corte de servicio en forma interna o a los clientes.

Arbor Networks® TMS

Las políticas de AIF del TMS les brindan a las organizaciones información detallada sobre ataques DDoS para que comiencen a bloquearlos de manera rápida y segura. Esta precisión es fundamental para bloquear ataques maliciosos que pueden generar costoso tiempo de inactividad. La AIF brinda este mismo nivel de protección al producto ASR 9000 vDDoS Protection de Cisco.

Desglose de la fuente de inteligencia

Hay dos suscripciones disponibles para la AIF: Estándar y Avanzada. Con dos suscripciones, los clientes pueden elegir el nivel de detección de ataques y/o la protección que se adapte a sus necesidades.

AIF Estándar

Con la fuente estándar, los clientes pueden detectar y/o solucionar algunos de los ataques más prevalentes dirigidos hoy en día contra las empresas, lo que incluye malware, botnets y ataques DDoS. Las políticas y tácticas defensivas se actualizan con nueva información sobre ataques para proveer una detección amplia y precisa. A continuación se incluyen algunos ejemplos de las políticas y las tácticas defensivas que incluyen esta fuente.

	Tipos de política de amenazas		APS	Spectrum	SP	TMS+
Comando y control	• Par a par • HTTP • IRC		✔	✔	✔	
Amenazas de reputación de DDoS	• Atacante • Objetivo		✔	✔	✔	
Malware	• Webshell • Ransomware • RAT • Antivirus falso • Bancos • Moneda virtual • Spyware • Drive By • Red social	• Bot DDoS • Dropper • Fraude publicitario • Gusano • Robo de credenciales • Backdoor • Exploit Kit • Punto de venta • Otros	✔	✔	✔	
Ubicación geográfica de IP	• Identificación por país para sources de tráfico entrante • Identificación por país para destinos de tráfico saliente		✔	✔	✔*	✔*
RegEx de DDoS	• Identifica atacantes de DDoS basado en indicadores de dirección IP de ATLAS • Identifica objetivos de DDoS basado en indicadores de ATLAS HTTP Flooder		✔			✔
Identificación de Web Crawler	Identifica conexiones entrantes a servicios web desde motores de búsqueda conocidos		✔			
ET Pro	Firmas IDS			✔		

Figura 2 *Ejemplos de amenazas identificadas usando la fuente AIF Estándar. Todas las tácticas defensivas y las políticas se actualizan continuamente, así que la lista anterior puede cambiar en cualquier momento.*

Cómo Arbor Networks tiene una posición única para resolver amenazas avanzadas

Arbor tiene una larga historia en investigación de botnet y mitigación de DDoS.

Debido a que las DDoS han evolucionado desde una simple táctica de diversión hasta una función de malware y botnets usados en crímenes cibernéticos y ataques de APT, Arbor ha expandido su equipo ASERT y sus capacidades de investigación para identificar y analizar tipos de amenazas adicionales. El enfoque de ASERT a la inteligencia de amenazas ahora incluye varios factores que no solo identifican amenazas, sino que confirman su persistencia y gravedad. Estos incluyen:

- Supervisión de reputación y rastreo activo de campañas de ataques basados en indicadores del mundo real provenientes de Red Sky Alliance.
- Un rico sistema de fondo para análisis de malware compuesto tanto de tecnología externa de socios como de análisis y procesos construidos internamente.

ASERT usa estos datos y análisis de amenazas para desarrollar la AIF, la cual es usada por los clientes de Arbor para detectar eventos que ocurren en la red, sobre ella o su alrededor. La combinación de esta microvisión (en la red) y macrovisión del tráfico de Internet (brindada a través del portal de ATLAS) les da a los clientes una clara ventaja para resolver amenazas avanzadas.

* *Ubicación geográfica de IP actualizada en SP, TMS y productos ASR 9000 DDoS Protection de Cisco por medio de parche de producto.*

* *Las políticas de AIF usadas en el TMS son las mismas que para la ASR 9000 DDoS Protection de Cisco.*

AIF Avanzada

La AIF Avanzada está diseñada para organizaciones a las que les preocupan los ataques sigilosos y más sutiles. Por medio de una suscripción a esta fuente, los clientes obtienen todas las tácticas defensivas y las políticas incluidas en la fuente Estándar; y también políticas adicionales para descubrir conductas que indican ataques continuados y de estilo campaña, que están muy personalizados para una empresa específica y son difíciles de detectar porque tienen aspecto de legítimos. A continuación hay ejemplos de tácticas defensivas y políticas que se incluyen en esta suscripción.

	Tipos de política de amenazas	APS	Spectrum	SP	TMS
Amenazas basadas en ubicación	• Servicios de anonimato de tráfico • TOR • Proxies • Sinkholes • Scanners • Otros	✔	✔		
Amenazas de correo electrónico	• Spam • Phishing	✔	✔		
Ataques dirigidos	• APT • Hactivismo • RAT • Watering Hole • Rootkits	✔	✔		
Móviles	• C&C móvil • Spyware • Apps maliciosas	✔	✔		

Figura 3 *Ejemplos de amenazas identificadas usando la fuente AIF. Las tácticas defensivas y las políticas se actualizan continuamente, así que la lista de arriba puede cambiar en cualquier momento dado. Las políticas de la suscripción Avanzada no están disponibles actualmente para clientes de SP, TMS o ASR 9000 DDoS Protection de Cisco.*

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: +57.1.508.7099
nola@arbor.net

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

www.arbornetworks.com

DS/AIF/SP/0717-LETTER