Fuente de inteligencia ATLAS®

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

FUNCIONES Y BENEFICIOS CLAVE

Actualizaciones dinámicas para una protección precisa
La AIF se actualiza en forma continua 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 fuentes 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.

Las amenazas a la seguridad pueden tomar muchas formas —desde redes caídas hasta uso no autorizado para robo de datos—, y los negocios de hoy no deben bajar la guardia contra atacantes que están fuertemente organizados y tienen muchos recursos. Una buena inteligencia de amenazas es fundamental para mantener el ritmo de los atacantes y minimizar o eliminar el riesgo que representan. Una buena inteligencia de amenazas permite que los profesionales de la seguridad tomen decisiones con confianza y actúen sobre las amenazas que descubren. Una buena inteligencia de amenazas otorga poder a los equipos de seguridad para que exploren más profundamente dentro de cada amenaza, descubran riesgos más grandes y constituyan un activo más importante para el negocio.

Tratar las amenazas avanzadas

La fuente de inteligencia ATLAS, o AIF (Atlas Intelligence Feed) de Arbor Networks, equipa a los clientes con políticas y tácticas defensivas que les permiten abordar ataques rápidamente como parte de una amenaza avanzada. La AIF es un servicio del Arbor Security Engineering and Response Team (ASERT) y permite a los clientes beneficiarse directamente de la capacidad y experiencia 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 o las amenazas avanzadas de los tiempos modernos. La mejor manera de proteger a su organización contra las amenazas es tener la inteligencia más actualizada desde la visión más amplia, enriquecida por veteranos expertos. Y esto es la fuente de inteligencia ATLAS.

La dinámica de una fuente de inteligencia de amenazas efectiva

Una inteligencia de amenazas efectiva requiere tres cosas:

- Una fuente 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 gestione todo lo que se menciona arriba 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. Una inteligencia de amenazas excelente requiere integración fluida en su programa de seguridad, lo que a su vez significa que la información debe ser procesable y válida. El riesgo de cada amenaza debe ser claro, y las acciones que hay que tomar deben ser evidentes.

ARBOR® NETWORKS
The Security Division of NETSCOUT

¿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 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.

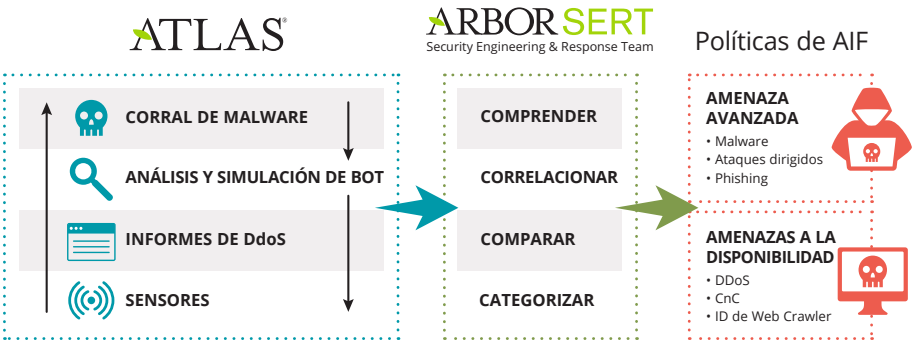

Figura 1: *ATLAS usa varias herramientas y procesos para recopilar y analizar datos de amenazas. El equipo se enfoca en las capacidades y el potencial de los ataques, y extrae varios indicadores de una campaña de ataques. Dichos indicadores se envían a los productos Arbor por medio de la Fuente de Inteligencia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

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 sobre 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 clave 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 específicos han estado en peligro. Se agrega 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 en los productos de Arbor bajo la forma de un puntaje de confianza, para que los usuarios puedan estar seguros de que una amenaza específica 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 fuente, las políticas incluirán 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 que están diseñados para hacer.

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 fuente 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

CÓMO ARBOR NETWORKS TIENE UNA POSICIÓN ÚNICA PARA RESOLVER AMENAZAS AVANZADAS

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

Pero a medida 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 ahora incluye varios factores que no solo identifican amenazas, sino que confirman su persistencia y gravedad. Estos incluyen:

- Sociedades valiosas como la Red Sky Alliance, que provee acceso a más de 23 millones de computadoras personales que se supervisan activamente en busca de inteligencia de amenazas.
- 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, sobre o alrededor de la red. 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.

fundamentales, con el contexto y la información para escalar eventos a fin de investigar con mayor detalle.

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 DDoS 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 denegación de servicio. Las políticas y tácticas defensivas se actualizan constantemente 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 se incluyen en 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 fuentes 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			✓		

* 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.

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 de arriba puede cambiar en cualquier momento.*

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 • App. 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

Sede corporativa
76 Blanchard Road
Burlington, MA 01803 EE. UU.
Llamada gratuita en los
EE. UU.: +1 866 212 7267
Tel.: +1 781 362 4300

www.arbornetworks.com

Ventas en Latinoamérica
Brasil
Tel.: +55.11.4380.8035
brasil@arbor.net
México, Caribe y América Central
Tel.: +52.55.4624.4842
mxcca@arbor.net
América Latina del Norte
Tel.: +57.1.508.7099
nola@arbor.net
América Latina del Sul
Tel.: +54.11.5218.4007
sola@arbor.net

DS/AIF/ES/1016-LETTER