IDC VENDOR SPOTLIGHT

Mejores prácticas Anti DDoS: un enfoque híbrido

Noviembre, 2017

Carlo Dávila y Marcelo Leiva

Patrocinado por: Arbor Networks, The Security Division of NETSCOUT

Ataques, tales como Mirai y WannaCry, han puesto al descubierto la fragilidad a nivel mundial de los sistemas de seguridad de las organizaciones que no se adecuaron a los nuevos retos relacionados con ecosistemas digitales. La perspectiva es que estos ciberataques sigan a la alza, especialmente los tipo DDoS, impulsados por el desarrollo acelerado de proyectos de transformación digital en las organizaciones, que están abriendo nuevos puntos de acceso a sus redes con la utilización de soluciones como la nube y el Internet de la Cosas (IoT). La utilización de dichas tecnologías puede potencialmente cambiar el perfil de riesgo de las organizaciones e incrementar su exposición a los ataques, si es que no se conjuga con una estrategia de seguridad avanzada.

Para reducir estos riesgos, la industria de seguridad de TI ha desarrollado soluciones y servicios avanzados que permiten responder y mitigar los potenciales ataques ejecutados en plataformas externas que van más allá del control de la organización.

Este documento describe el actual escenario de los ataques DDoS, sus proyecciones de crecimiento, la situación de América Latina y cómo las soluciones híbridas, entre sistemas de protección on premise y en la nube, se ubican como una de las mejores prácticas para combatir estos riesgos. Se analiza la oferta de soluciones de Arbor Networks y sus retos para fortalecer su presencia en la región.

I. INTRODUCCIÓN

El año 2016 fue para IDC un punto de inflexión en la estrategia de seguridad para cualquier organización al revelarse el tamaño que pueden alcanzar los ataques distribuidos de denegación de servicio (DDoS) –tales como el ataque del código malicioso Mirai en octubre del 2016–, explotando las vulnerabilidades en dispositivos inteligentes y en otros dispositivos conectados a Internet.

La conclusión detrás de las acciones del ataque de Mirai contra un proveedor de Internet en Estados Unidos, y las del Ransomware llamado WannaCry en 2017, es que las actividades de los ciberdelincuentes se incrementarán en los próximos años. Esto se debe a los bajos niveles de seguridad de TI con los que se están diseñando y ejecutando los proyectos de tecnología basados en el Internet de la Cosas (IoT), la nube, la movilidad y otros aceleradores de innovación que soportan los procesos de la transformación digital dentro de las organizaciones.

El incremento en el número de ataques DDoS ha sido progresivo. Por ejemplo, entre los ataques DDoS que detectó la firma de seguridad Arbor Networks en 2016, el mayor de ellos alcanzó un nivel de 800 gigabits por segundo (Gbps); esto es, 60% más que el año anterior, cuando se registraron acciones de 550 Gbps de acuerdo con el XII reporte de seguridad Arbor WISR WW Infrastructure Security Report 2016.

En el 2016 se documentó un ataque DDoS de 579 Gbps, que equivalía a descargar casi 250 mil documentos por segundo contra un objetivo en el Reino Unido.

De ahí la importancia de que las organizaciones revisen y replanteen sus estrategias de seguridad de Tecnologías de la Información (TI), identificando sus posibles vulnerabilidades y reforzando sus soluciones para mitigar estos ataques. En dicha revisión, las compañías necesitan entender que las nuevas amenazas han rebasado las capacidades de las soluciones tradicionales de ciberseguridad, por lo cual deben considerar soluciones de seguridad avanzadas para ubicar la mejor alternativa de acuerdo con el perfil de riesgo de la organización, y bajo qué esquema les conviene adquirirlas.

II. DEFINICIONES

Como parte del desarrollo del presente documento, se incluyen las siguientes definiciones:

- Ataques DDoS

En términos sencillos, IDC explica que se trata de una acción delictiva que utiliza un botnet (un grupo de dispositivos infectados y conectados a Internet) y consultas DNS, u otros medios, para enviar requerimientos de comunicación malintencionados a otros equipos de una red. La finalidad es saturar el sitio web y /o la red denegando el servicio a usuarios legítimos (Worldwide DDoS Prevention Products and Services Forecast, 2017-2021).

Pero, en los últimos años los ataques se han sofisticado y especializado, por lo que actualmente los ataques de DDoS se clasifican como sigue:

- Volumétricos. Intentan consumir el ancho de banda ya sea dentro de la red o servicio objetivo; o bien, entre la red y el servicio de Internet provocando una congestión.
- De agotamiento. Intentan consumir las tablas de estado de conexión presentes en diversos componentes de la infraestructura, tales como los balanceadores de carga, firewalls, IPS y los propios servidores de aplicaciones. Pueden incluso inutilizar dispositivos de alta capacidad habilitados para mantener millones de conexiones.
- A nivel de capa de aplicación. Se dirigen hacia algún aspecto de una aplicación o servicio en la capa 7 de la red. Son los ataques más sofisticados, furtivos y los más difíciles de detectar.

- Soluciones Anti-DDoS

De acuerdo con la taxonomía de IDC, las soluciones anti DDoS detectan y mitigan los ataques distribuidos de denegación de servicio. Poseen un nivel de especialización mayor a los que se ofrece en los firewalls, IPS y otros productos de seguridad, al responder no solo a los ataques volumétricos, sino también a amenazas más sofisticadas que explotan los huecos de seguridad en los dispositivos e infraestructura de la red de las organizaciones (IDC's Worldwide Security Products Taxonomy, 2016).

Dichos productos pueden adquirirse de diversas maneras, ya sean integrados a un dispositivo en la red, en licencias de software, como servicio en la nube, e incluso en un modelo híbrido, que combina una solución *on premise* y en la nube para combatir con mayor eficacia un ataque contra la infraestructura de la organización.

III. TENDENCIAS

Los ataques en 2016 y 2017 mediante botnet basados en Mirai dejaron claro que las organizaciones, de cualquier tamaño, país o industria, pueden ser víctimas potenciales de estos ataques, y que las acciones criminales se intensificarán, especialmente con los proyectos de IoT.

Arbor Networks reporta que en los últimos años los ataques DDos han alcanzado niveles de 800, 600, 550 y 500 Gbps, y que la frecuencia de los mismos se incrementó en 53%, con más de 50 ataques mensuales en promedio. Sin embargo, con un ataque de 1 Gbps, los atacantes pueden saturar la conectividad a Internet de la mayoría de las organizaciones. El impacto podría ser la interrupción del servicio, pérdida de ingresos y el daño a la reputación de la empresa, a menos que cuenten con la protección contra ataques DDoS, de acuerdo con el reporte Arbor WISR WW Infrastructure Security Report 2016.

En América Latina, Brasil fue el país más atacado, ubicándose en el octavo lugar a nivel global. El resto de los países no fue la excepción, con incrementos importantes en el número de ataques DDoS.

Los principales objetivos de los ataques DDoS en 2016, de acuerdo con el estudio de Arbor Networks, son los proveedores de acceso a Internet, instituciones de gobierno, empresas del sector financiero, de servicios de hospedaje, manufactura y servicios en general, e incluso usuarios finales.

Factores que impulsan el crecimiento de los ataques DDoS

El rápido crecimiento de los ataques se debe a varios factores, uno es la facilidad de acceso en línea a las herramientas para lanzar un ataque DDoS. Por un poco de dinero, o incluso gratuitamente, se obtienen metodologías de ataque creadas por hackers experimentados y que son utilizadas de manera esporádica durante años.

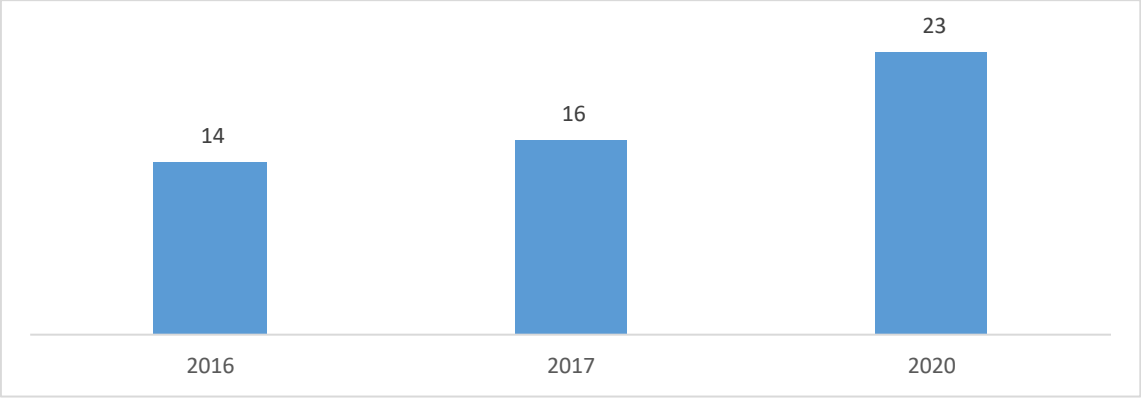
Otro factor es el incremento de la vulnerabilidad de las organizaciones derivado de los proyectos de innovación en las empresas, que involucran soluciones de cómputo en la nube, movilidad, IoT y otros aceleradores de innovación como impresión 3D y robótica, entre otros. Esto se debe a la falta de medidas de seguridad específicas para ataques DDoS, lo que es una situación aprovechada por los ciberdelincuentes.

Proyecciones del mercado de anti DDoS

Debido al crecimiento de los ataques y la difusión de los mismos en los medios de comunicación, las empresas están reaccionando con un incremento en la demanda de soluciones especializadas anti DDoS. A nivel mundial, IDC espera que el mercado total de estos productos y servicios tenga una tasa mundial de crecimiento anual compuesto de 20.7% del 2016 al 2021; en el caso de América Latina, la estimación es más conservadora con un crecimiento promedio anual de 13% entre 2015 y 2020.

FIGURA 1

Latam- Soluciones DDoS en millones de dólares



Fuente: IDC Latin America, DDoS Solutions, 2016

IV. BENEFICIOS

Idealmente, las empresas deben integrar desde sus proyectos de innovación las soluciones avanzadas de seguridad que les permitan reducir los riesgos por la integración de un mayor número de componentes a su red. Los sistemas anti DDoS, brindan una solución multifacética para detectar y bloquear ataques al combinar varias tácticas defensivas. Y ofrecen una visibilidad integral del tráfico de la red y de las actividades potencialmente peligrosas.

Hoy día, los proveedores están agregando varias capas para mitigar los ataques de denegación de servicio para mejorar sus defensas tanto en redes como en aplicaciones: firewalls avanzados de aplicación web (WAF) y defensas específicas de SSL. Otros son los dispositivos de mitigación de DDoS en sitio que trabajan con motores para clasificar el tráfico "malo" del "bueno", que típicamente incluyen otras funcionalidades como seguimiento de amenazas y análisis de comportamiento.

Una empresa puede utilizar estos dispositivos y desarrollar su técnica propia para mitigar los posibles ataques. Además, existe la oferta de servicios administrados por parte de diferentes proveedores de servicios.

Otra opción es el enfoque híbrido: la integración de una solución desplegada *on premise* en la empresa, con un servicio en la nube administrado por algún proveedor de servicios de seguridad, de hosteo o Internet, entre otros. Los componentes *on premise* en la organización proporcionan visibilidad de los ataques a la red, antes de que el sistema en la nube los detecte. Si no se pueden contener los ataques, se redirecciona el tráfico a la nube de manera automática y se lanza una alerta antes de que los recursos de la compañía se agoten.

Esta oferta logra una plena integración e intercambio de información entre los componentes de la solución; acelera los esfuerzos de mitigación, aumenta la eficiencia, brinda una mayor visibilidad de las situaciones de riesgo, e incluye ayuda especializada para mitigar las amenazas. Para IDC las soluciones híbridas pueden ser la mejor alternativa para la protección de las organizaciones, ya que presentan una propuesta de protección más extensa.

V. ARBOR NETWORKS, OFERTA Y RETOS EN EL MERCADO

Arbor Networks, The Security Division of NETSCOUT, es un proveedor de seguridad avanzada de redes con casi 17 años de experiencia en el mercado. Es una división de NETSCOUT que ofrece soluciones de visibilidad de redes, detección y mitigación de DDoS, contrarrestando campañas de malware y botnets. Se especializa en la protección de la infraestructura y el ecosistema de Internet.

El enfoque de la empresa se basa en el estudio detallado del tráfico de red, al considerar que la seguridad en las organizaciones se concentra en esta infraestructura, además de ser la fuente para el claro entendimiento de los ataques y las acciones rápidas para mitigarlos. La compañía hace énfasis en que no trabaja sobre amenazas o ataques específicos ni en puntos en la red, sino en las redes en sí mismas.

Sus principales clientes en el mundo y América Latina son los operadores de servicios de telecomunicaciones, proveedores de seguridad administrada, servicios en la nube, redes sociales, así como también empresas financieras, entidades de gobierno y educación.

Su oferta contra los ataques y amenazas DDoS se conforma de visualizadores de red, sistemas dentro de la red empresarial, y una solución híbrida respaldada por un centro de investigación del tráfico de Internet.

- Sistemas de visibilidad de la red
  - SP puede ser un software, dispositivo o servicio virtual para operadores que ofrece una visibilidad generalizada con facilidad. Analiza paquetes, Netflow, rutas SNMP y BGP en toda la red, transformando datos en información, lo que permite a las empresas tomar medidas con base en dicha información para solucionar sus problemas comerciales, desde la planificación y el diseño de la red hasta la detección y mitigación de amenazas.
  - Spectrum integra la visibilidad a escala de Internet y la detección de amenazas avanzadas para las redes empresariales. Se diseñó para que los equipos de seguridad lo utilicen para la detección de amenazas avanzadas, ya que permite a los especialistas conectar indicadores de ataques globales a las actividades dentro de la red.

- Solución en sitio
  - APS es la oferta para las organizaciones que provee protección anti DDoS, incluyendo los ataques contra la capa de aplicación. Analiza las amenazas y proporciona recomendaciones personalizadas de mitigación de ataques DDoS, conocidas como emergentes. Sus medidas incluyen un conjunto de protecciones basadas en paquetes, que neutralizan la gran mayoría de las amenazas de botnet globales. El sistema se actualiza automáticamente con las estrategias de seguridad proporcionadas por el Equipo de Ingeniería de Seguridad y Respuesta de Arbor Networks; genera reportes de ataque en tiempo real y a profundidad junto con la mitigación de DDoS forense, el cual detalla hosts bloqueados, países de origen de los ataques y las tendencias históricas.

- Sistema híbrido
  - Cuando surge un ataque volumétrico grande y se sobrecargan los circuitos, una de las principales formas de ataques DDoS en el mundo, la empresa tiene una solución combinada entre el APS del cliente y la nube de Arbor Networks para realizar una mitigación automatizada. Arbor Cloud es un servicio global de protección contra ataques DDoS totalmente administrado e independiente del proveedor de servicio de Internet, que posee una capacidad de mitigación de más de 4 Tbps. Cuenta con el respaldo de un centro de operaciones de seguridad, que se encuentra activo las 24 horas del día, y el equipo de Ingeniería de Seguridad y Respuesta de la empresa.

- Centro de investigación del tráfico de Internet
  - ATLAS es un proyecto de colaboración con casi 330 clientes, básicamente proveedores de servicios, quienes acordaron compartir datos de tráfico anónimos por hasta 140 Tbps – cerca de un tercio del tráfico mundial–, lo que permite al centro de investigación de Arbor Networks contar con información sobre los DDoS, malware y botnets que amenazan la infraestructura del Internet y la disponibilidad de la red. La información es monitoreada y analizada para reforzar las soluciones y servicios de la compañía contra estas amenazas.

El enfoque de esta firma para el desarrollo de negocios está basado en un modelo de canales de valor agregado, bajo un programa de socios de negocios diferenciado para el mercado de Infraestructura de Service Providers y el mercado Enterprise. Su objetivo es brindar el soporte adecuado a los usuarios finales de la región. Actualmente, Arbor Networks cuenta con un programa de certificación sin costo, fondeo de mercadotecnia conjunta, y apoyo en generación de demanda, incluyendo una política de protección del negocio.

Arbor Networks tiene una oferta muy específica para ataques DDoS, que cubre hasta las amenazas en la capa de aplicaciones de las redes, una de las más complejas de detectar. Incluye su oferta híbrida entre Availability Protection System (APS) y Arbor Cloud, y sus centros de investigación en tiempo real que analizan el tráfico de Internet en el mundo, lo que le permite tener un panorama global del desarrollo y avance de las amenazas. Este conocimiento se aplica en sus soluciones para impedir que los ataques tengan acceso a las redes de sus clientes.

Retos en Latin America

Impulsar la adopción de estas tecnologías, en especial en América Latina, conlleva retos que Arbor Networks y, en general, los proveedores de estas soluciones necesitan revertir: la falta de información sobre las nuevas amenazas y la resistencia de algunas organizaciones a reconocer el impacto real que los ataques DDoS pueden tener en el negocio. Debido a esto, muchas organizaciones siguen confiando únicamente en dispositivos desplegados on premise, que no son necesariamente especializados para enfrentar ataques de perfil DDoS. También hay organizaciones que tienen defensas integradas, acordes a estrategias tradicionales o que se enfocan únicamente en acciones contra ataques volumétricos.

La falta de conocimiento especializado en las empresas agrega la diversidad en la oferta y precios de las soluciones. De ahí que resulta importante un enfoque de seguridad estratégico para reducir los riesgos y mitigar los ataques DDoS con la solución a la medida a sus necesidades, y el presupuesto óptimo para su nivel de riesgo.

El mercado requiere de una oferta de soluciones generadas con base en la situación de América Latina, donde los directivos deben tomar decisiones difíciles sobre lo que está sucediendo ahora y lo que podría ocurrir en el futuro, tomando en cuenta que sus presupuestos continúan reduciéndose. Bajo este contexto, invertir en un modelo de servicios o uno híbrido, podría estar más alineado a las necesidades de las organizaciones de Latinoamérica.

VI. CONCLUSIONES Y RECOMENDACIONES

En Latinoamérica, los ataques de DDoS presentaron crecimientos exponenciales en menos de un año (2015 a 2016); tal es el ejemplo de Ecuador. La tendencia es un aumento en las acciones de los ciberdelincuentes en los siguientes años, por lo que consideramos que la situación se agrava en la región debido la reducción que hubo en las inversiones en TI y seguridad en los últimos años, producto de la crisis económica del 2015.

Tenemos también un aumento en los proyectos de innovación en las empresas que incluyen soluciones en la nube, movilidad y/o IoT, los cuales incrementan puntos potenciales de riesgo de ataques DDoS si no se establece una estrategia de seguridad contra amenazas avanzadas, tales como las generadas por los botnets basados en Mirai.

Para reducir los riesgos es necesario que las organizaciones:

- Revisen sus políticas y estrategias de seguridad de acuerdo con los cambios en sus ecosistemas de TI y el nivel de riesgo asociado a cada industria.
- Hagan un análisis para identificar sus posibles vulnerabilidades y comprender que las nuevas amenazas han rebasado las capacidades de las soluciones tradicionales de ciberseguridad.
- Ubiquen cuáles son las mejores alternativas para mitigar sus potenciales riesgos, de acuerdo con el perfil de la organización, y determinen bajo qué esquema deben adquirir las soluciones.
- Consideren las soluciones híbridas anti DDoS como una de las alternativas más completas con las que pueden abarcar el espectro de las amenazas actuales y de tendencia en un futuro, especialmente para los ataques de volumen masivo.

Ante este escenario, IDC ha identificado que las empresas de América Latina invertirán cada vez más en soluciones anti DDoS, como lo muestran las proyecciones de crecimiento de 13% en promedio entre 2015 y 2020, y este incremento se dará a partir de una mayor educación y concientización de las organizaciones sobre los "nuevos" riesgos potenciales que pueden enfrentar.

También será importante que las empresas reciban servicios de consultoría por parte de los proveedores de soluciones para crear estrategias de seguridad. Los usuarios buscan cada vez más ofertas flexibles y fáciles de integrar a la infraestructura de TI, adecuadas al mercado latinoamericano, especialmente sensible al tema de costos. Las demostraciones de cómo las soluciones de un proveedor especializado en DDoS ayudarían a reducir y mitigar estos ataques serán muy relevantes al momento de evaluar opciones.

Es necesario tomar en cuenta que los ciberdelincuentes van "un paso adelante" respecto a la concepción de las empresas usuarias sobre las acciones de prevención y mitigación de riesgos, pues a menudo se piensa que las soluciones tradicionales de seguridad son suficientes para protegerse contra los ataques DDoS y no se considera la inversión en soluciones especializadas.

Finalmente, los servicios de consultoría para los directivos TI y la organización pueden contribuir en el diseño y justificación de soluciones de defensa en profundidad o híbridas, de acuerdo con las necesidades de la industria y el negocio. La oferta debe contar con diferentes niveles de servicios de mitigación, mediante pago mensual o bajo demanda, a precios competitivos para reducir la barrera de los costos, y que así puedan estar al alcance de cualquier tamaño y tipo de empresa.

Acerca de IDC

International Data Corporation (IDC) es la principal firma mundial de inteligencia de mercado, servicios de consultoría, y conferencias para los mercados de Tecnologías de la Información, Telecomunicaciones y Tecnología de Consumo. Durante más de 50 años, IDC ha venido ayudando a los profesionales de TI, ejecutivos de negocios y la comunidad de inversión, a tomar decisiones fundamentadas sobre la compra de tecnología y la estrategia de negocios. Más de 1,100 analistas proveen conocimiento global, regional y local sobre las oportunidades de la industria y las tendencias de tecnología en más de 110 países alrededor del mundo. IDC es una subsidiaria de IDG, empresa líder en tecnología, investigación y eventos.

IDC Latinoamérica

4090 NW 97th Avenue Suite 350,
Doral, FL, USA 33178
+1-305-351-3020
Twitter: @IDCLatin
www.idclatin.com
www.idc.com