



**LOCALHOST**  
soluciones innovadoras

## Detección y Mitigación de Ataques de Denegación de Servicio Distribuidos (DDoS)

# Qué es un Ataque de Denegación de Servicio?

Un Ataque de Denegación de Servicio, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios que realizan transacciones y/o acceden en forma legítima. Normalmente provoca la pérdida de la conectividad de la red de acceso del cliente, por el consumo excesivo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

"Un intento de agotar recursos finitos, explotar debilidades en diseños o implementaciones o de explotar falencias de capacidad de infraestructura".

Un ataque se genera mediante la saturación intencional de los puertos con flujo de información, haciendo que los recursos se sobrecarguen y no puedan seguir prestando servicios, por eso se le dice "denegación", pues hace que los servidores no tengan capacidad de responder a los usuarios que acceden en forma legítima. Esta técnica es usada por los llamados hackers para dejar fuera de servicio a servidores objetivo.

"Afecta la disponibilidad y utilidad de recursos de red".

Una ampliación del ataque DoS es el llamado Ataque Distribuido de Denegación de Servicio, también llamado ataque DDoS (de las siglas en inglés Distributed Denial of Service) el cual se lleva a cabo generando un gran flujo de información desde varios puntos de conexión.

"El daño colateral causado por un ataque puede ser tan malo (sino peor) que el ataque en sí mismo".  
aque puede ser tan malo (sino peor) que el ataque en sí mismo".

# Cómo se gesta un ataque DDoS?

## Se identifican cuatro etapas diferenciadas:

### 1 EL ENCARGO

El interesado en sabotear un sitio web se pone en contacto con un pirata informático al que le encarga la acción a cambio de dinero.



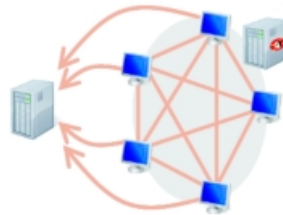
### 2 PUESTA EN MARCHA

El pirata desde cualquier parte del mundo activa un programa que controla miles de PC "Zombis" sin que sus dueños lo sepan.



### 3 ARMADO DEL EJERCITO

Estos "Zombis" mandan ordenes a otras PC reflectores para que saturen con peticiones a la web a atacar.



### 4 EL ATAQUE

Los reflectores realizan por oleadas peticiones masivas y sincronizadas al servidor, lo saturan y como consecuencia, el servicio cae.



## Y se presenta un escenario de Escalamiento de Amenazas de DDoS


- › El número de vulnerabilidades de seguridad explotables continúa incrementándose.
- › La conectividad de banda ancha para individuos es ahora algo muy común (DSL, Cable etc..)
- › Las herramientas de ataque automatizadas están disponibles de manera pública y no se requiere una gran técnica para emplearlas.
- › La sofisticación de los ataques se está volviendo más pronunciada, evadiendo las técnicas de detección manual.
- › La motivación para los atacantes varían con su razonamiento malicioso.

# Plataforma en LocalHost Tecnología Líder en el mundo

El datacenter implementó una plataforma de tecnología líder a nivel mundial, correspondiente al Proveedor ARBOR. El producto comercial se denomina Peakflow.

## ARBOR Peakflow® SP

### Quién es ARBOR?

- › Fundada en el año 2000
- › Más de 160 Empleados
- › Presencia en 10 Países
- › Más de 200 Clientes
- › Socios Estratégicos  
Con ISP ya afianzados en el mercado y con relaciones en crecimiento desde el año 2000  
Fingerprint Sharing Alliance tiene más de 50 miembros
- › Presencia Global  
Productos implementados en más del 70% de los ISP del mundo  
ATLAS (atlas.arbor.net) 



# Tipos de Ataques DDoS que cubre el Servicio de LocalHost

El servicio desarrollado por el Datacenter proporciona detección, análisis y mitigación de eventos DDoS para clientes específicos y su infraestructura, usando técnicas de detección de anomalías. 4/5

**La red permite detectar ataques, mediante el monitoreo continuo y permanente del tráfico cursado, en base a:**

- › Variaciones del perfil de tráfico
- › Patrones coincidentes con los registros de worms, virus, etc.
- › Mal uso de protocolos, paquetes mal formados
- › Escaneo de puertos y direcciones no utilizadas

Existen numerosos mecanismos mediante los cuales se causa una denegación de servicio. El servicio que ofrece LocalHost contempla la detección de

Tipo de Ataque	Descripción
<i>Spooferd</i>	Envío de paquetes con una dirección de origen falsificada
<i>Malformed</i>	Envío de paquetes con bits o flags encendidos en forma anormal
<i>Floods</i>	Envío de paquetes conformados de manera legítima en gran cantidad
<i>Null</i>	Envío de paquetes sin contenido
<i>Protocol</i>	Envío de paquetes con protocolos ilegítimos
<i>Fragmented</i>	Envío de paquetes fragmentados los cuales nunca serán completados
<i>Brute Force</i>	Envío de paquetes que exceden el umbral definido de 'flow rates'

Respecto de cualquier otro tipo de ataque recibido por el Cliente que no sea de los indicados en el cuadro precedente, LocalHost realizará sus mejores esfuerzos por detectarlo y mitigarlo, sin garantizar ni comprometer su identificación y / o filtrado.



# Operación del Servicio que brinda LocalHost

La prestación de LocalHost se circunscribe al monitoreo permanente y continuo de los patrones y perfiles de tráfico del Cliente, lo que permitirá la detección en forma temprana, de un ataque de Denegación de Servicio Distribuido (Distributed Denial of Service - DDoS) proveniente de los enlaces internacionales de internet que vinculan a la Red IP de LocalHost.

A tal fin se utilizará una plataforma de tecnología líder en el mercado, que permite la detección, análisis y reportes de eventos de esta naturaleza.

Mediante la infraestructura instalada en la red de LocalHost, un operador, en forma proactiva identifica los potenciales ataques provenientes de los vínculos internacionales de Internet, en 5/5 base a la correlación de distintas técnicas de análisis que proveen las herramientas de monitoreo correspondientes a la plataforma de detección.

Una vez identificado el ataque, el operador de LocalHost comunicará la Alarma de Ataque al responsable designado por el cliente, quién deberá informar la decisión de no mitigar.

El Cliente deberá notificar a LocalHost su decisión de no mitigación, y en tal caso LocalHost no realizará acción alguna sobre el tráfico a Internet del cliente. Caso contrario se especificará la decisión de realizar la mitigación y LocalHost procederá con la misma.

En caso de que el responsable facultado del cliente no sea ubicable o no especifique la decisión de no mitigación, LocalHost procederá con el proceso de mitigación.

# Beneficios

Reducción del tiempo de respuesta para mitigar eventos de DDoS, minimizando los daños directos y periféricos del ataque.

La continuidad operativa del sitio del Cliente con tráfico legítimo, preserva el desarrollo del negocio del Cliente vinculado a los recursos que fueran afectados por tráfico malicioso (ej transacciones por ventas on-line, transacciones de Internet banking, medios de comunicación /información on-line).

La resolución de problemas de DDoS se ejecuta "en la nube" por personal experto en infraestructura de ruteo del Datacenter, por lo que la amenaza no afecta el ancho de banda de los recursos de acceso del cliente.

Facilita a los clientes la toma de decisiones urgentes sobre sus esquemas de seguridad.

Reduce el riesgo de problemas de interoperabilidad.