

# - Evitar ataque de DDoS de Anonymous, entre otros - 17/09/2011

Autor: [Lic. Cristian F. Borghello](#)

[www.segu-info.com.ar](http://www.segu-info.com.ar)

*Los ataques de Denegación de Servicio Distribuidos (DDoS por sus siglas en inglés) siempre han sido una pesadilla para los administradores de IT y seguridad y desde la popularización de este tipo de ataques por parte del grupo Anonymous, utilizado como su principal herramienta de "protesta", miles de organizaciones públicas y privadas de todo el mundo han tenido que comenzar a pensar seriamente en alternativas para detectar, mitigar y/o bloquear la tormenta de tráfico desatada por estos ataques.*

*Algunos ejemplos de estos ataques recientes se pueden encontrar en el Blog de Segu-Info:*

- <http://blog.segu-info.com.ar/search/?q=anonymous>
- <http://blog.segu-info.com.ar/search/?q=DDoS>

*En forma general, un ataque de Denegación de Servicio (DoS por sus siglas en inglés) [1] se genera mediante la saturación o sobrecarga de un servicio o recurso, de forma tal que el mismo deja de responder, lo hace en forma intermitente o más lento que de lo normal.*

*Un ataque de DDoS se produce cuando cientos o miles de computadoras se conectan a un servicio y, como el servidor no es capaz de responder a cada una de las solicitudes deja de responder (denegación) y se vuelve inaccesible para los posibles usuarios legítimos. Generalmente las conexiones y ancho de banda consumido provoca la pérdida de la conectividad de la red de la víctima.*

*La eficiencia del ataque se basa en la cantidad de atacantes y en el ancho de banda utilizado por cada uno de ellos. En un [ejemplo publicado por Microsoft](#) suponen lo siguiente:*

- *se tienen 500 máquinas atacantes*
- *cada una de ellas tiene una conexión DSL y utiliza un ancho de 128 Kb/seg. (de subida)*

*Con esto se puede generar  $500 * 128 \text{ Kb/seg.} = 64000 \text{ Kb/seg.} = 62,5 \text{ MB/seg.}$  Esto es aproximadamente el tamaño de 40 líneas T1 (1,544 MB/seg.). Por supuesto variando el número de atacantes y su ancho de banda promedio, se producen cambios en el volumen de tráfico y así se podría inundar fácilmente redes de cualquier tamaño.*

*Si bien el ataque más conocido y realizado en la actualidad es al servicio web, se puede realizar sobre cualquier recurso de la víctima, desde el correo electrónico (e-mail bombing), tiempos de procesamiento, espacio de almacenamiento, teléfono, fax, etc.*

*La saturación simplemente obedece a afectar de alguna forma la ejecución normal de tareas por parte del afectado, lo cual finalmente impacta en su imagen y en los beneficios del negocio.*

*En caso de una entidad pública o gubernamental este tipo de ataques puede afectar seriamente a las operaciones que la entidad brinda a los ciudadanos y por eso se utiliza como medio de reclamo y protesta ya que el impacto es público, masivo y multiplicador.*

*NOTA: es importante destacar que existen otros tipos de ataques de DDoS más sofisticados y/o efectivos [2] pero que quedan fuera de este artículo por no ser utilizados masivamente por Anonymous o por no "estar al alcance" de un usuario normal.*

*En la actualidad estos ataques se pueden realizar de diversas maneras pero se destaca el uso y alquiler de Botnet: la infección de miles de usuarios permite utilizar esos recursos como herramienta de ataque por parte de un delincuente en el momento que se desee. Básicamente cualquier usuario, infectado por un troyano del tipo Bot, puede formar parte de un ataque dirigido a una organización y, sin saberlo ser "cómplice" de la comisión de delitos con alcance internacional.*

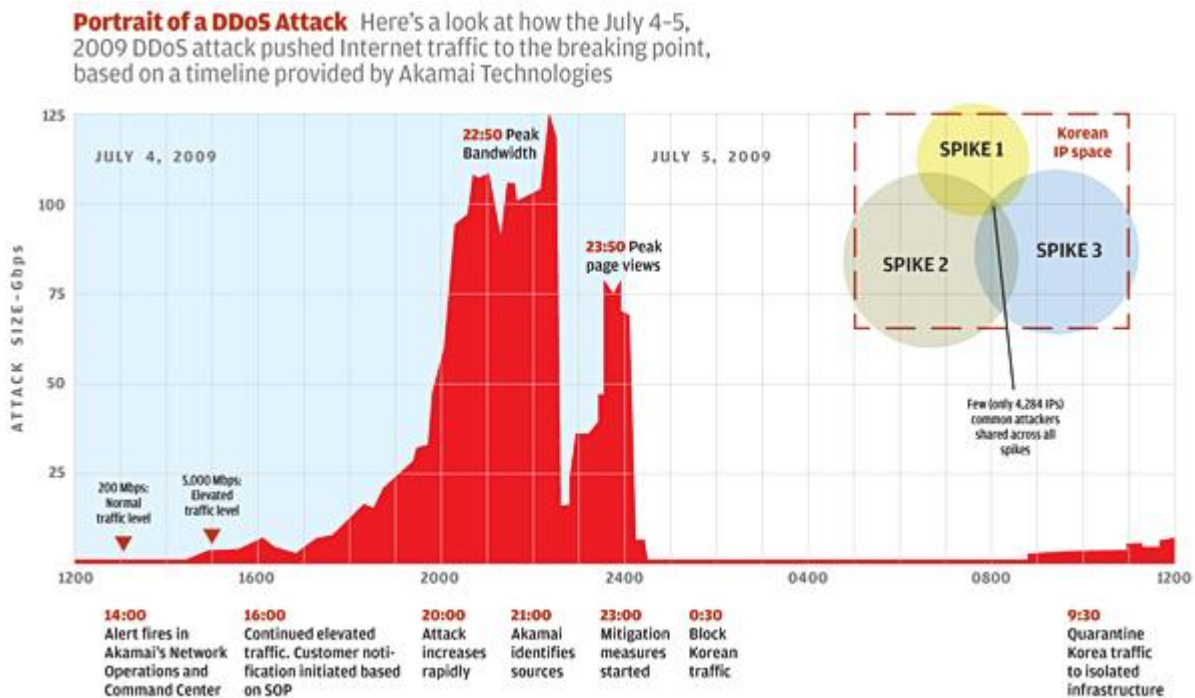
*Por otro lado se ven potenciados y facilitados por el uso de herramientas (point-and-click) diseñadas para tal fin y sin ningún nivel de sofisticación. Este es el caso de las aplicaciones Open-Source HOIC (High Orbit Ion Cannon) y LOIC (Low Orbit Ion Cannon) [3] publicadas por parte de Anonymous y que, a través de canales IRC, coloca los ataques de DDoS al alcance de cualquier usuario sin conocimientos para que "se puedan realizar reclamos de manera masiva", como aquellos contra diversas empresas privadas (Visa, MasterCard, PayPal, Amazon, etc.) en el caso Wikileaks a finales de 2010 y contra organismos públicos de diferentes países en los últimos meses.*

*A través del uso de las herramientas mencionadas, todos los participantes del ataque realizan miles de conexiones HTTP (peticiones GET) TCP/UDP hacia los servidores víctimas, de modo que el servicio web deja de responder. La cantidad de atacantes necesarios dependerá del ancho de banda y recursos del servidor atacado, yendo de pocos cientos en el caso de un servidor de una PyME, a miles, en el caso de servicios de alta disponibilidad.*

*Cuando muchos o todos los usuarios cesan el ataque (o cierran la aplicación), el servicio se restablece, en teoría, sin ningún tipo de acción por parte de los administradores ni de daño físico ni lógico a los servidores de la organización.*

En otros casos de ataques extremos, como el realizado contra [WordPress en marzo](#), "se enviaron varios gigabits y decenas de millones de paquetes por segundo", lo cual podría obedecer a varios factores, desde la motivación política, el uso de herramientas gratuitas y, la combinación de Botnet con varios miles de usuarios infectados.

En la siguiente imagen de Akamai, puede verse claramente la forma en que el tráfico impacta en los servidores, lo que sucede cuando se toman las medidas de bloqueo y mitigación y cuando finaliza el ataque.



Paradójicamente, las herramientas propuestas por Anonymous no son anónimas y lo que muchos "atacantes casuales" ignoran es que [la dirección IP de quien utiliza estas herramientas es visible y se encuentra expuesta](#). Esto posibilita el rastreo por parte de las organizaciones víctimas y de las autoridades.

Para evitar este tipo de rastreo muchos usuarios se decantan por el uso de Proxies (como TOR y otros), ignorando que en realidad en este caso la denegación de servicio se está realizando sobre el proxy utilizado.

Por eso Anonymous ya promociona (supuestamente para este mes de septiembre) la publicación de una nueva herramienta posiblemente llamada "RefRef" [4] y que usaría JavaScript y SQL para atacar los sitios y aprovecharse de sus vulnerabilidades, además de que podría ser utilizada desde cualquier dispositivo, incluyendo smartphones.

Una vez conocido el impacto de los ataques de DDoS es necesario conocer los controles disponibles y que se pueden implementar para contrarrestar este tipo de ataques.

Comenzando por el caso más simple en que se desee implementar un nuevo servicio web, se podría considerar [Lighttpd](#), un web-server para entornos \*NIX muy liviano y concebido desde la seguridad y el cual es utilizado, por ejemplo, por YouTube y Wikipedia.

En servidores web ya implementados con tecnología LAMP, se puede considerar la implementación de BSD PF [5] y [Linux NetFilter/Iptables](#) para controlar el tráfico TCP/IP, limitar el ancho de banda disponible, realizar una inspección de paquetes a través de las capas del modelo OSI (Stateful Packet Filtering), entre otras muchas funcionalidades.

Teniendo en cuenta que cualquiera puede ser víctima de un DDoS (sin importar el tamaño de la organización o la red), dependiendo de los servicios brindados, los recursos disponibles y las herramientas utilizadas por parte de los atacantes, se podría considerar los [siguientes puntos](#):

- Limitar de 50 a 100 el número de conexiones desde un origen determinado. Si se trata de un ataque, las conexiones excedentes se eliminarán (drop).
- Limitar de 5 a 10 el número de conexiones realizadas por segundo.
- Bloquear/Ignorar temporal o definitivamente las direcciones IP identificadas como posibles atacantes.
- Perfeccionar las técnicas de Ingress-Filtering de modo de poder "identificar como no-anomalías" las direcciones IP que solicitan un recurso. Se puede consultar la [RFC 2827](#) que define dichas políticas.
- Para evitar ataques de tráfico saliente desde una organización (como por ejemplo desde una botnet) también se debe considerar las políticas de Egress-Filtering, solicitada en varias disposiciones y regulaciones vigentes, como [PCI DSS](#).

Algunos ejemplos de configuración de estas herramientas pueden ser encontrados en [Lighttpd Traffic Shaping](#), [PF firewall](#) y [Linux Iptables](#).

En entornos Microsoft, existe una serie de consejos y guías que deben ser adoptados [6] e incluyen desde la modificación de ciertos parámetros del registro hasta la instalación y configuración de los servidores de IIS, ISA, Exchange y Forefront TMG. En estas configuraciones se pueden observar y modificar los valores y límites por defecto de cada solicitud de conexión.

Por otro lado, si bien la mayoría de los dispositivos de networking actuales pueden ser configurados para bloquear muchos tipos de ataques clásicos, si se trata de ataques de DDoS orientado y masivo, se deben aumentar las medidas preventivas, con el consecuente aumento considerable de costos.

Por ejemplo la empresa Arbor, especializada en el estudio y combate de este tipo de ataques dice que sus aparatos "están diseñados para detectar los ataques volumétricos en el rango de los varios GB/seg." [7].

*Otras empresas como [RioRey](#), [F5](#), [Corero](#), [IntruGuard](#), [Cisco](#), [Watchguard](#), [TippingPoint](#) y [Checkpoint](#) ofrecen soluciones similares con montos que pueden ascender a varios cientos de miles de dólares dependiendo del ancho de banda soportado. En rangos similares de costos, se ubican también los [servicios de protección DDoS basados en la nube](#), en donde se suele pagar por ancho de banda consumido durante los ataques.*

*NOTA: CloudFlare [8] es un servicio de Cloud que brinda protección de DDoS en forma gratuita (también tiene un servicio pago) y que puede ser utilizado por cualquier particular o empresa de desee evaluar este tipo de alternativas.*

*Evidentemente los ataques de DDoS seguirán entre todos los usuarios y las organizaciones por mucho tiempo más y es hora de comenzar a pensar en si nuestra organización ya se encuentra preparada para afrontarlos, porque el ciberterrorismo y la ciberguerra ya están entre nosotros y deberemos decidir de qué lado jugar.*

*[1] DoS y DDoS en Wikipedia*

*<http://es.wikipedia.org/wiki/Ddos>*

*<http://en.wikipedia.org/wiki/Ddos>*

*[http://en.wikipedia.org/wiki/Denial-of-service\\_attack](http://en.wikipedia.org/wiki/Denial-of-service_attack)*

*[2] Tipos de Ataques de Denial of Service (DoS)*

*[Amenazas Lógicas - Tipos de Ataques - Denial of Service \(DoS\)](#)*

*[Global Information Assurance Certification Paper](#)*

*[3] Herramientas HOIC, LOIC y d0zme*

*[D0z.me Please, un acortador de URL que genera DDoS](#)*

*[Análisis de HOIC y LOIC, las herramientas usadas para los DDoS](#)*

*[4] RefRef de Anonymous*

*[Anonymous está desarrollando una nueva arma de ataque](#)*

*[Anonymous may be testing a new attack tool dubbed #RefRef](#)*

*[5] BSD PF (Packed Filter)*

*[PF: The OpenBSD Packet Filter](#)*

*[PF: El filtro de paquetes de OpenBSD](#)*

*[6] Protegerse de DDoS en entornos Microsoft*

*<http://technet.microsoft.com/es-ar/library/cc700847.aspx>*

*<http://technet.microsoft.com/es-ar/library/cc750607.aspx>*

*<http://technet.microsoft.com/en-us/library/cc722931.aspx>*

*<http://technet.microsoft.com/en-us/library/cc750213.aspx>*

<http://technet.microsoft.com/en-us/library/bb794735.aspx>  
<http://technet.microsoft.com/en-us/library/dd897007.aspx>  
<http://technet.microsoft.com/es-ar/library/ee207140.aspx>  
[Microsoft Forefront TMG Behavioral Intrusion Detection](#)

[7] *Arbor Networks*

[Arbor Networks](#)

[Data center anti-DDoS package on tap from Arbor](#)

[8] *CloudFlare, una posible solución frente a ataques DDoS*

[CloudFlare, Inc.](#)

[CloudFlare, una posible solución frente a ataques \(D\)DoS](#)