Ataques DDoS, desde los tipos hasta las técnicas utilizadas

El nacimiento de IoT se ha convertido en un multiplicador de fuerza para los ataques DDoS En Internet, los piratas informáticos y activistas prefieren los ataques de denegación de servicio distribuido (DDoS). Así lo demuestran numerosos casos recientes, que han confirmado el crecimiento del fenómeno. Esto se debe a la facilidad de uso de las herramientas para su gestión. Además, la llegada del Internet de las cosas (IoT) ha simplificado el trabajo y ha multiplicado exponencialmente los efectos.

Las botnets que explotan el IoT, de hecho, han demostrado ser el arma perfecta y un multiplicador de fuerza ideal, siguiendo la escasa o inexistente protección de los dispositivos y al mismo tiempo su conectividad. Los ataques DDoS también han llamado la atención de la prensa internacional, que cada vez más aborda el tema o denuncia ciberincidentes de este tipo.

Los tipos de ataque DDoS

El término DDoS, sin embargo, es genérico. Existen diferentes tipos de agresión con esta técnica. El primero son los ataques basados en volumen. Estos utilizan mucho tráfico para inundar el ancho de banda de la red. Además, existen «protocolos» que se centran en explotar los recursos de un servidor. Finalmente, están las «aplicaciones», dirigidas contra aplicaciones web. Estos se consideran los tipos de ciberataques más sofisticados y peligrosos.

Reflexión / Amplificación 101

Uno de los tipos de ataques DDoS más populares que se emplean en la actualidad es el ataque de reflexión / amplificación, que permite a los atacantes generar ataques de mayor volumen mediante la combinación de dos métodos:

- En los ataques de reflexión, los adversarios falsifican la dirección IP de un objetivo y envían una solicitud de información, principalmente utilizando el Protocolo de datagramas de usuario (UDP) o, en algunos casos, el Protocolo de control de transmisión (TCP). Luego, el servidor responde a la solicitud, enviando una respuesta a la dirección IP del objetivo. Esta «reflexión», que utiliza el mismo protocolo en ambas direcciones, es la razón por la que se denomina ataque de reflexión. Cualquier servidor que opere servicios basados en UDP o TCP se puede apuntar como reflector.
- Los ataques de amplificación generan un gran volumen de paquetes que se utilizan para saturar el sitio web de destino sin alertar al intermediario. Esto ocurre cuando un servicio vulnerable responde con una gran respuesta cuando el atacante envía su solicitud, a menudo llamado paquete de activación. Usando herramientas fácilmente disponibles, el atacante puede enviar muchos miles de estas solicitudes a servicios vulnerables, lo que genera respuestas que son considerablemente más grandes que la solicitud original y amplifican significativamente el tamaño y el ancho de banda emitidos al objetivo. La amplificación puede incluir múltiples paquetes de respuesta a un solo paquete, o paquetes de mayor tamaño que el original. Cualquiera de los métodos da como resultado una amplificación.
- Un ataque de reflexión / amplificación combina los dos, lo que permite a los atacantes aumentar la cantidad de tráfico malicioso que pueden generar y ocultar las fuentes del tráfico del ataque. Las formas más

frecuentes de estos ataques se basan en millones de DNS, NTP, SNMP, SSDP y otros servicios basados en UDP / TCP expuestos.

Las técnicas: desde SYN Flood hasta Ping of Death

Los tipos de ataques DDoS también se dividen en categorías, según la cantidad de tráfico involucrado y las vulnerabilidades objetivo. Los más comunes son los «SYN Floods», que se dirigen a las debilidades en la secuencia de conexión TCP (el triple protocolo de enlace). Luego están las «inundaciones UDP», vinculadas al Protocolo de datagramas de usuario. A estos se suman los «HTTP Flood», que utilizan menos ancho de banda que otros ataques, pero obligan a los servidores a utilizar el máximo de recursos. Ping of Death manipula los protocolos IP enviando pings maliciosos a un sistema. Esta técnica fue muy popular hace años, pero hoy se considera obsoleta e ineficaz.

De Smurf Attack a Slowloris

El «Smurf Attack» es un ataque DDoS que utiliza IP y el Protocolo de mensajes de control de Internet (ICMP). Para ello, utiliza un malware llamado smurf. Fraggle Attack utiliza una gran cantidad de tráfico UDP, que envía a la red de transmisión del enrutador. Es similar al tipo de agresión anterior, pero en lugar de ICMP usa UDP. El «Slowloris» permite a los atacantes utilizar recursos mínimos durante un ciberataque contra un servidor. Una vez conectado al objetivo, hace que la conexión permanezca abierta el mayor tiempo posible, a través de la inundación HTTP. Se ha utilizado en varios casos de ataques DDoS conocidos. Incluida la de 2009 con motivo de las elecciones presidenciales iraníes.

Desde ataques a nivel de aplicación hasta días cero

Los ataques a nivel de aplicación aprovechan las vulnerabilidades de las aplicaciones. Su objetivo no es afectar a todo el servidor, sino solo a sus partes débiles. NTP Amplification ”aprovecha los servidores Network Time Protocol (NTP), que se utilizan para sincronizar relojes. El DoS persistente avanzado (APDoS), por otro lado, es utilizado por los piratas informáticos para causar daños graves. Utiliza diferentes variedades de ataques DDoS y apunta a múltiples vectores, que envían millones de solicitudes por segundo. Los ataques APDoS pueden durar meses, dependiendo de la habilidad del creador. Para mantenerlos en pie, de hecho, puedes cambiar de táctica y crear desviaciones para evadir las defensas del objetivo. Por último, los ataques DDoS de «día cero» se centran, según su nombre, en vulnerabilidades que aún no se han parcheado.

Leer también: ¿Qué es un sistema de prevención de intrusiones, IPS? ; Informática forense, qué es, definición, significado;

Supervisión de infraestructura: desafíos y mejores prácticas