Proxies Anónimos Son Usados Para Los Ataques Escopeta DDoS

En cierto momento nos ha de preocupar nuestra privacidad y la huella que dejamos en el Internet. No es de extrañar que más de nosotros estemos recurriendo a proxies anónimos para ocultar nuestras IP y los detalles HTTP.

Pero una nueva investigación de la compañía de seguridad Incapsula ha descubierto un lado más oscuro para el uso de anonimizadores como **fuente de ataques DDoS**.

De acuerdo con los ataques DDoS de proxies anónimos representaron el 20 por ciento de todos los ataques a nivel de aplicación. En promedio, los autores estaban dirigiendo el tráfico de 1.800 IPs diferentes. Esto es lo que Incapsula llama un **ataque de «Shotgun» o escopeta**.

La idea detrás de este tipo de ataque es **utilizar un gran número de proxies abiertos**, enfocando a una negación de una sola fuente de servicio (DoS) en uno distribuido (DDoS), lo que hace que sea mucho más difícil de mitigar. También es atractivo para los atacantes, ya que hace que sean más difíciles de rastrear.

Los atacantes obtienen una **lista de servidores proxy** de acceso público, mediante un script o herramientas de lista disponibles en línea. A continuación, utilizan una versión modificada de un conjunto de herramientas DoS o un script hecho en casa para enviar un lote de solicitudes maliciosos a través de cada uno de los proxies cosechados.

Esto produce un efecto de dispersión, similar a las pequeñas bolitas de un cartucho de escopeta, de ahí el nombre. Sin embargo, cuando los perdigones se dispersan, el DoS siempre

da en el mismo objetivo; golpeándola desde múltiples direcciones, creando un ataque DDoS.

El gráfico siguiente muestra la distribución de un DDoS escopeta en comparación con la de un ataque convencional de tamaño similar. Con proxies anónimos, el ataque no sólo se puede propagar a través de varias direcciones IP, sino también a través de múltiples ubicaciones geográficas, por lo que las técnicas de bloqueo por geo localización es ineficaz.

El informe muestra que casi el **45 por ciento de todos los ataques DDoS escopeta** se originó de IPs de la red Tor. De ellos, el 60 por ciento se realizó a través de la herramienta Hammer DoS tool. Los proxies anónimos promediaron 540.000 solicitudes por ataque.