CENTRO CIBERNÉTICO POLICIAL

B@CISP – 01 | Boletín de Análisis Criminal en CIBERSEGURIDAD ISP

Ataques DDOS a ISP

Los ataques de amplificación DDoS basados en DNS (Domain Name System), se han incrementado en los últimos meses, apuntando a routers domésticos vulnerables. Un simple ataque puede crear decenas de Gbps de tráfico para interrumpir las redes de los proveedores de servicio, empresas, páginas web e individuos de cualquier parte del mundo usando técnicas de amplificación DNS, reflexión NTP (Network Time Protocol) o una combinación de ambas.

Misión de nuestro servicio en línea CAI VIRTUAL

La Policía Nacional en su rol misional debe garantizar la ciberseguridad de los colombianos, en materia de prevención, atención y judicialización del cibercrimen.

CENTRO CIBERNÉTICO POLICIAL

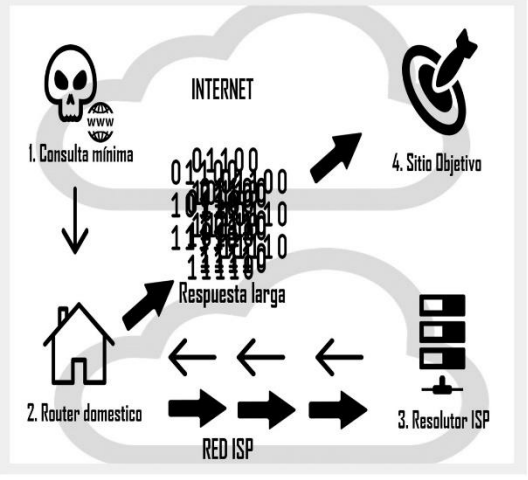
B@CISP – 01 Boletín de Análisis Criminal en CIBERSEGURIDAD ISP

¿Como funciona?

En un nivel muy simple, el ataque DDOS satura a un router con tantas peticiones que este colapsa y se vuelve inservible, estos ataques son usados como distractores mientras otros ataques ocurren de manera simultanea (Sqlljection, Replay, CeroDay, etc).

Por otra parte, los routers domésticos vulnerables enmascaran el blanco de un ataque, es difícil para los ISP determinar el destino final y el receptor de grandes oleadas de tráfico amplificado. El tráfico procedente de los ataques de amplificación interrumpen las redes de los ISP, sitios web y a individuos. El impacto en los ISP es más significativo debido a:

- Impacto en la red generada por el tráfico malicioso al saturar el ancho de banda disponible.
- Impacto en los ingresos debido a la pérdida de clientes o a gastos para retenerlos, por un ineficiente servicio de Internet.
- Impacto en la reputación debido a que el tráfico no deseado se dirige hacia otros proveedores.



Recomendaciones

Para asegurar que la solicitud que se obtiene como respuesta a una consulta de URL es correcta o si por el contrario es manipulada, el CCP recomienda como solución a largo plazo para el envenenamiento de caché DNS, el uso de DNSSEC (Domain Name System Security Extensions).

DNSSEC permitirá a las organizaciones firmar sus registros DNS, usando criptografía de clave pública, asegurando que su equipo sabrá si un registro DNS debe ser de confianza o si ha sido envenenado y redirige a una ubicación incorrecta.