RECOMENDACIONES

Por todo ello se recomienda estar prevenidos ante ataques DDoS aplicando las siguientes medidas preventivas específicas:

- Activación de restricción por geolocalización de dirección IP
- Bloquear aquellas peticiones HTTP maliciosas que provienen de las herramientas utilizadas por los atacantes, cuya firma es la siguiente: "Accept: text/html,application/xhtml+xml,application/xml," (especial atención a la coma del final que determina que es maliciosa)
- Activación de planes de contingencia para mitigación de DDoS.

Por otro lado, se recomiendan las siguientes medidas más generales:

- Refuerzo de la monitorización en sistemas críticos y servicios expuestos a Internet.
- Aplicación de parches y actualizaciones en todos los equipos y servidores.
- Comunicación inmediata ante cualquier incidente sospechoso a CSIRT-CV.