

Alerta ID:	108
Fecha del reporte:	06/06/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Campaña de ataques de denegación de servicio distribuido (DDoS) contra entidades del Estado colombiano
Herramienta de detección	N/A
Activo involucrado:	Gobierno / Entidades del Estado (con relevancia para el sector salud)
Tipo de alerta:	Boletín Alerta
Nivel de riesgo:	Media-Alta

Resumen ejecutivo

Informar a las entidades del sector salud monitoreadas por el CSIRT Salud sobre la actividad hacktivista del grupo “Dark Storm Team”, el cual ha reivindicado ataques de denegación de servicio distribuido (DDoS) contra portales del Gobierno Nacional —incluido el Ministerio de Salud y Protección Social—. El boletín tiene como propósito describir el modus operandi del actor, entregar los indicadores de compromiso (IoC) y el mapeo MITRE ATT&CK asociados para su monitoreo, y proporcionar recomendaciones de detección y mitigación que permitan fortalecer preventivamente la disponibilidad de los servicios expuestos a Internet, ante un eventual aumento del rango de objetivos del grupo.

Descripción:

A través del canal de Telegram **t.me/Darkstormteam22**, el grupo hacktivista autodenominado “Dark Storm Team” publicó una serie de mensajes en los que se atribuye ataques DDoS contra los portales web de cuatro carteras del Gobierno Nacional colombiano: **Ministerio de Transporte, Ministerio de Trabajo, Ministerio de Salud y Protección Social y Ministerio de Agricultura**. En la publicación, cada entidad aparece marcada con un símbolo de “caído” (X)



acompañado de enlaces al servicio **check-host.net**, herramienta de comprobación de disponibilidad ampliamente utilizada por actores de DDoS para evidenciar la indisponibilidad de un objetivo.

Dark Storm Team es un grupo hacktivista activo desde finales de 2023, especializado en ataques DDoS de gran escala contra portales gubernamentales, infraestructura crítica y grandes plataformas digitales (se le atribuyó la caída global de la red social X —antes Twitter— en marzo de 2025). El grupo organiza y difunde sus operaciones a través de Telegram y foros, recluta simpatizantes, ofrece servicios de DDoS bajo demanda (DDoS-as-a-Service) y, en algunos casos, comercializa datos filtrados. Durante 2025 se observó un giro de sus campañas hacia portales gubernamentales y del sector público.

La motivación de Dark Storm Team es principalmente **ideológica**: de orientación propalestina y con narrativas alineadas a intereses prorrusos, dirige sus ataques contra entidades que percibe como afines a Israel o adversarias de Rusia. A ello se suma un componente de **notoriedad e intimidación** (reivindicación pública y reclutamiento) y un componente **lucrativo** (servicios de DDoS bajo demanda y venta de datos). Sus oleadas suelen coincidir con coyunturas geopolíticas, fechas simbólicas o declaraciones políticas.

La inclusión de Colombia y Ecuador en sus listados sugiere una expansión hacia la región andina. En ese marco, cualquier coyuntura mediática o postura del país percibida como afín a Israel podría detonar nuevas oleadas contra entidades del Estado, incluido el sector salud. La siguiente valoración resume el riesgo:

Dimensión	Valoración	Justificación
Probabilidad	Media	El grupo ya incluyó a MinSalud en su listado y muestra expansión regional; sin embargo, el sector salud no es históricamente su objetivo prioritario.
Impacto	Medio-Alto	Indisponibilidad de portales y servicios al ciudadano; el DDoS por sí solo no compromete la confidencialidad de la información.
Riesgo (prob. x impacto)	Medio-Alto	Amerita monitoreo activo y preparación de mitigación, sin requerir respuesta de máxima criticidad salvo confirmación de escalamiento.



Como parte de la reivindicación, el grupo difundió un reporte de **check-host.net** (enlace check-report/413b4540ka51) correspondiente al portal del Ministerio de Salud y Protección Social.

Los datos del reporte son:

Campo	Valor
Sitio evaluado	https://www.minsalud.gov.co/
Dirección IP del objetivo	181.61.204.233 (Colombia, Bogotá)
Fecha y hora de la comprobación	Sábado 6 de junio de 2026, 13:11:23 UTC
Resultado	La mayoría de los nodos de verificación distribuidos a nivel global (Europa, América, Asia y Medio Oriente) reportan "Connection timed out", sin código de respuesta HTTP

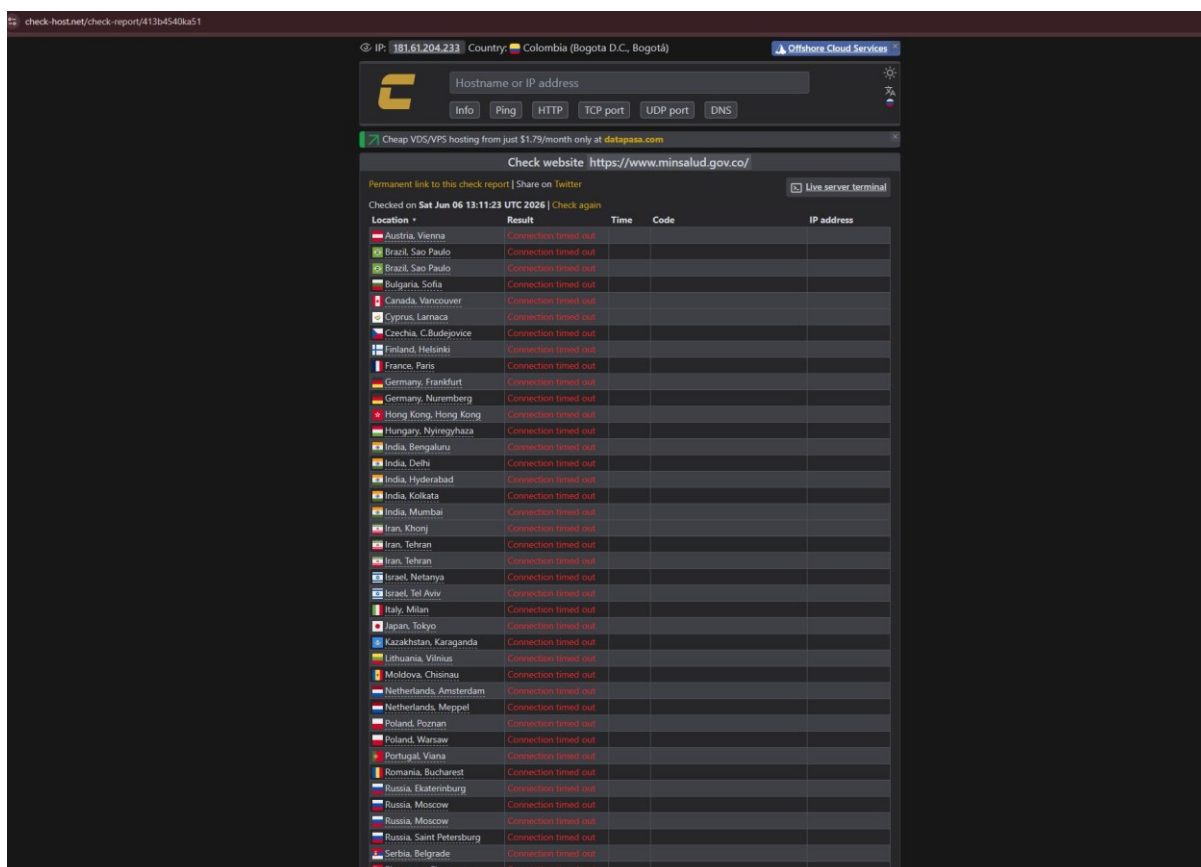


Figura 1. Reporte de check-host.net difundido por el actor (captura).



Un resultado de “Connection timed out” desde múltiples nodos internacionales indica que, en el momento de la comprobación, el sitio no respondió a las solicitudes de esos puntos de verificación. No obstante, **este reporte por sí solo no constituye prueba concluyente de un ataque DDoS exitoso**, ya que el mismo patrón puede originarse por causas distintas.

Histórico de ataques del grupo.

Desde su aparición tras el 7 de octubre de 2023, Dark Storm Team ha mantenido una actividad sostenida de ataques DDoS contra objetivos de alto perfil. A continuación se resumen los hechos más relevantes reivindicados por el grupo:

Fecha	Objetivo / hecho	Tipo
Ago. 2023	Creación del canal de Telegram del grupo	Infraestructura
Oct. 2023	Tras el 7 de octubre: ataques a un hospital, al gobierno, municipios e industrias sensibles en Israel	DDoS
15 oct. 2023	Aeropuerto Internacional John F. Kennedy (JFK), Nueva York — EE. UU.	DDoS
18 oct. 2023	Snapchat	DDoS
Feb. 2024	Aeropuerto Internacional de Los Ángeles (LAX) — EE. UU.; ultimátum a países OTAN, Israel y aliados	DDoS / amenaza
2024–2025	Infraestructura crítica: Puerto de Haifa (Israel) y Ministerio de Defensa de EAU	DDoS
10 mar. 2025	Plataforma X (antes Twitter): caídas globales del servicio	DDoS
Abr. 2025	Foro de cibercrimen BreachForums (varias oleadas)	DDoS
2025	Giro hacia portales gubernamentales y del sector público, con foco en Europa	DDoS
2025–2026	Expansión hacia Latinoamérica: reivindicación de ataques contra entidades del Estado de Ecuador	DDoS
Jun. 2026	Reivindicación de ataques contra ministerios del Gobierno de Colombia	DDoS (en verificación)

Nota: el histórico se basa en reivindicaciones del propio grupo y en reportes de inteligencia de fuentes abiertas (OSINT); no todos los hechos han sido confirmados de forma independiente.



Sectores y países afectados

Aunque su motivación es ideológica, el grupo ha mostrado un patrón de objetivos amplio. Los principales sectores afectados a lo largo de su historia son:

Sector	Ejemplos / observaciones
Transporte y aeropuertos	Foco recurrente del grupo: aeropuertos JFK y LAX (EE. UU.)
Gobierno y administración pública	Sitios y servicios gubernamentales; foco creciente durante 2025
Infraestructura crítica	Puertos (Puerto de Haifa), energía y defensa (Ministerio de Defensa de EAU)
Servicios financieros	Instituciones financieras en los países objetivo
Tecnología y redes sociales	Plataformas digitales como Snapchat y X (antes Twitter)
Salud	El primer ataque conocido del grupo se dirigió a un hospital
Educación	Instituciones del sector educativo
Medios de comunicación	Medios y servicios informativos

Países afectados: Israel, Estados Unidos, países miembros de la OTAN, Ucrania, Emiratos Árabes Unidos, Egipto, Francia, Italia, Países Bajos, Tailandia y, recientemente, entidades del Estado de Ecuador y Colombia. La actividad reciente en Ecuador y Colombia evidencia una expansión del grupo hacia la región andina, lo que incrementa la exposición de las entidades del país

Relevancia para el sector salud: si bien las campañas del grupo se concentran en gobierno, transporte e infraestructura crítica, su primer ataque conocido se dirigió a un hospital y el listado más reciente incluye al Ministerio de Salud y Protección Social de Colombia. Por ello, las entidades del sector salud no deben considerarse fuera de su rango de objetivos.



Consecuencias de la explotación

Un ataque DDoS exitoso o sostenido contra la infraestructura de una entidad puede acarrear, entre otras, las siguientes consecuencias:

- Indisponibilidad total o parcial de portales y servicios web expuestos a Internet, con impacto directo en la prestación de servicios al ciudadano.
- Degradación del rendimiento (lentitud y errores intermitentes) aun cuando el servicio no caiga por completo.
- Afectación reputacional y de la confianza institucional.
- Posible uso del DDoS como cortina de humo (distracción) para encubrir intentos de intrusión, exfiltración o despliegue de otras amenazas en paralelo.
- Saturación de recursos de red, servidores y appliances perimetrales (firewalls, balanceadores), pudiendo afectar también servicios internos.
- Costos operativos asociados a la respuesta, mitigación y recuperación del servicio.

Indicadores de compromiso del grupo (IoC)

Por tratarse de ataques de denegación de servicio, las direcciones IP de origen son **efímeras y frecuentemente falsificadas (spoofed) o provenientes de proxies/botnets**, por lo que no se publican IP fijas como indicadores confiables. El monitoreo debe apoyarse en la huella OSINT del actor y en indicadores conductuales:

Tipo	Indicador	Observación
Canal de Telegram	t.me/Darkstormteam22	Canal de difusión y reivindicación de ataques
Alias del grupo	Dark Storm Team, DarkStorm, DarkStormTeam, TeamDarkStorm, MRHELL112	Identificadores usados por el actor



Tipo	Indicador	Observación
Herramienta de "evidencia"	Enlaces a check-host.net/check-report/...	Usada para demostrar la indisponibilidad del objetivo
Grupos asociados	Matryoshka 424, AlixSec, Mr. Hamza	Coaliciones y alianzas hacktivistas para campañas conjuntas
Indicador conductual	Picos abruptos de tráfico y alto volumen de peticiones HTTP/S desde múltiples orígenes hacia portales públicos	Patrón típico de DDoS volumétrico / de capa de aplicación

Indicadores tempranos de ataque (early warning)

Las siguientes señales pueden anticipar una oleada de ataques y permiten pasar de una postura reactiva a una preventiva:

- Publicación de listas de objetivos o amenazas en el canal de Telegram del grupo y de coaliciones aliadas (p. ej. Matryoshka 424).
- Menciones de la entidad, sus dominios, sus direcciones IP o del país en canales y foros hacktivistas.
- Incremento de actividad de reconocimiento: escaneo de puertos, fingerprinting de servicios web y picos de peticiones a rutas de descubrimiento.
- Ráfagas cortas de tráfico de "calentamiento" (warm-up) previas al ataque principal.
- Aumento de tráfico desde ASN, proxies o regiones geográficas inusuales hacia los portales públicos.
- Coyunturas geopolíticas o fechas simbólicas que históricamente han precedido oleadas del grupo.

Modo de explotación detallado.

A diferencia de la explotación de una vulnerabilidad de software, un ataque DDoS no aprovecha una "falla" puntual, sino que **abusa de la capacidad finita** de los recursos expuestos

pág. 7



(ancho de banda, conexiones, CPU de servidores y appliances). El ciclo de ataque observado en este tipo de actor comprende las siguientes fases:

Reconocimiento (Reconnaissance)

El grupo identifica portales y servicios públicos expuestos, mapea endpoints de alto valor (formularios, buscadores, descargas, APIs) que generen mayor consumo de recursos y evalúa la presencia de protecciones (CDN/WAF) para seleccionar los objetivos que producirán la mayor interrupción.

Preparación de infraestructura (Resource Development)

Empleo de botnets, servicios de “booter/stresser” y plataformas de DDoS-as-a-Service, junto con proxies y servidores VPS para distribuir geográficamente el origen del tráfico y dificultar el bloqueo.

Coordinación y reclutamiento

Convocatoria a través de Telegram, donde se publican los objetivos y se coordinan oleadas de tráfico con simpatizantes y grupos aliados (campañas conjuntas dentro de coaliciones hacktivistas).

Ejecución del ataque — vectores típicos

- **Ataques volumétricos (capa 3/4):** inundaciones UDP, ICMP y técnicas de amplificación/reflexión (DNS, NTP, etc.) orientadas a agotar el ancho de banda del enlace.
- **Ataques de protocolo (capa 4):** SYN flood, ACK flood y similares que agotan las tablas de estado de firewalls y balanceadores.
- **Ataques a la capa de aplicación (capa 7):** inundaciones HTTP/HTTPS (GET/POST flood) y peticiones repetidas a endpoints costosos, que agotan los recursos del servidor web/aplicación con relativamente poco tráfico.

El objetivo es lograr la máxima indisponibilidad con el menor costo posible, manteniendo el ataque de forma sostenida o por oleadas sucesivas.



Verificación

El grupo comprueba la indisponibilidad del objetivo mediante check-host.net y captura de pantallas como “prueba” del ataque.

Reivindicación y propaganda

Publicación de los resultados en Telegram con fines de notoriedad, intimidación del objetivo y reclutamiento de nuevos simpatizantes.

Relación con tácticas y técnicas MITRE ATT&CK

Táctica	Técnica (ID)	Descripción
Reconnaissance (TA0043)	Active Scanning (T1595)	Escaneo de bloques de IP y de vulnerabilidades para identificar objetivos y endpoints de alto impacto.
Resource Development (TA0042)	Acquire / Compromise Infrastructure: Botnet (T1583.005 / T1584.005)	Adquisición o uso de botnets, VPS y servicios de booter para originar y distribuir el tráfico de ataque.
Impact (TA0040)	Network Denial of Service (T1498)	Inundaciones volumétricas y de amplificación/reflexión (T1498.001 Direct Network Flood / T1498.002 Reflection Amplification) para agotar el ancho de banda.
Impact (TA0040)	Endpoint Denial of Service (T1499)	Agotamiento de recursos de SO, servicio y aplicación (T1499.001 a T1499.004), incluyendo HTTP flood en capa 7.

Recomendaciones

- Activar o validar servicios de mitigación DDoS upstream con el proveedor de Internet (ISP) o mediante CDN/scrubbing (p. ej. Cloudflare, Akamai o proveedor nacional), idealmente en modo “always-on” para los servicios críticos.



- Implementar y afinar el WAF con limitación de tasa (rate limiting), retos JS/challenge y reglas anti-bot para mitigar las inundaciones de capa 7.
- Habilitar control de conexiones, protección SYN-cookies y rate limiting en firewalls y balanceadores.
- Apoyarse en CDN y caché para absorber y dispersar el tráfico, ocultando además el origen real de los servidores.
- Considerar geobloqueo o listas de reputación de IP para tráfico claramente anómalo, con cautela para no afectar a usuarios legítimos.
- Disponer de un plan de respuesta a incidentes DDoS con roles, umbrales de activación, contactos del ISP/proveedor de mitigación y procedimiento de escalamiento (incluido blackholing/scrubbing).
- Mantener canales de comunicación alternativos para informar a la ciudadanía durante una eventual indisponibilidad.
- No interactuar con los enlaces de check-host.net ni con el canal de Telegram desde infraestructura institucional sin las debidas precauciones.
- Reportar de inmediato cualquier afectación al CSIRT Salud.

Inventario y priorización de activos expuestos

Como medida preventiva de fondo, se recomienda a cada entidad:

- Mantener un inventario actualizado de portales, aplicaciones web, APIs y servicios expuestos a Internet, identificando los críticos para la prestación del servicio al ciudadano.
- Clasificar y priorizar los activos según su criticidad y el impacto de una eventual indisponibilidad.
- Validar, para cada activo crítico, la protección anti-DDoS/WAF/CDN, la capacidad y redundancia, y la exposición innecesaria de puertos o servicios.
- Reducir la superficie de ataque: deshabilitar servicios innecesarios y ocultar las direcciones IP de origen detrás de un CDN.



FUENTES:



- Check Point Research — Perfil del grupo Dark Storm Team y ataque a la plataforma X (marzo de 2025).
- SecurityScorecard — Hacktivist Involvement in the Israel-Hamas War (histórico de objetivos del grupo).
- Orange Cyberdefense — Cyber Insight: DarkStorm Team (sectores y países objetivo).
- Cyble / Cybernews — Perfiles y cronología de actividad de Dark Storm Team (2023–2025).
- MITRE ATT&CK — T1498 (Network Denial of Service), T1499 (Endpoint Denial of Service), T1595 (Active Scanning), T1583/T1584 (Infraestructura: Botnet).
- Publicación del propio actor en el canal de Telegram t.me/Darkstormteam22 (imagen analizada).

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 3168931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

