Alerta ID:	43
Fecha del reporte:	10/10/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Indicadores de compromiso (IOC) - Direcciones IP publicas orígenes de tráfico malicioso
Herramienta de detección	FortiSIEM
Activo involucrado:	Direccionamiento IP público del Ecosistema Digital
Tipo de alerta:	Boletín informativo
Nivel de riesgo:	Crítico

Resumen ejecutivo

El CSIRT Salud ha identificado, a través de la plataforma SIEM, múltiples eventos de tráfico permitido desde una (1) dirección IP clasificada en listas negras (IPSum – malware/botnet) durante los últimos 7 días.

La criticidad de estos hallazgos es alta, ya que se observan intentos de conexión hacia direcciones IP públicas del sector, que no fueron bloqueadas y por lo tanto representan un riesgo de comunicación con infraestructura maliciosa.

Descripción del evento

Fuente de detección: SIEM sectorial.

Categoría: Tráfico permitido desde IPs maliciosas (IPSum).

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Severidad: Alta.

Patrón identificado: conexiones desde rangos asociados a malware, botnets y servidores de comando y control (C2).

Comportamiento observado: persistencia en intentos de conexión desde Rusia.

Plataformas donde están reportadas las IPs con mayor número de ataques

A continuación, se relaciona la dirección IP con sus correspondientes fuentes en donde fue verificada y corroborada como maliciosa.

Dirección Origen	Cantidad detectada	Fuente	URL Fuente
178.22.24.30	12560	AbuseIPDB	https://www.abuseipdb.com/check/178.22.24.30
		VirusTotal	https://www.virustotal.com/gui/ip-address/178.22.24.30
		AlienVault OTX	https://otx.alienvault.com/indicator/ip/178.22.24.30
		Shodan	https://www.shodan.io/host/178.22.24.30

Impacto Potencial

- Compromiso de seguridad de la red ya que esta IP están asociadas a botnets, malware C2 (command & control), proxies anónimos o servidores de ataque, lo que podría indicar que algún equipo interno está infectado y está reportando o recibiendo instrucciones desde un atacante.

- Exposición a intrusiones por lo que esta IP están documentadas por hacer escaneo de puertos ataques de fuerza bruta en RDP/SSH/HTTP, si algún equipo responde podría estar exponiendo servicios mal configurados o credenciales débiles.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Riesgo de fuga de información al tener uno o varios equipos del ecosistema Digital comprometidos podrían exfiltrar datos sensibles hacia esas IPs (credenciales, información de clientes, archivos internos).

- Pérdida de reputación / bloqueo para direcciones internas que podrían estar comunicarse con esas Ips maliciosas hacia internet pueden terminar también en listas negras lo que podría ocasionar emails rebotados o bloqueados.

Recomendaciones

- Bloquear de manera inmediata la dirección IP 178.22.24.30, tanto para el tráfico saliente como para el tráfico entrante. Si sigue activa podría estar generando mayor numero de ataques a las Entidades.
- Revisar los equipos que hayan sido destino o fuente de las conexiones dirigidas hacia esta dirección IP para descartar compromiso.
- Fortalecer las políticas de filtrado de tráfico perimetral, de forma que este tipo de conexiones no se permita sin un análisis previo.
- Mantener monitoreo constante en busca de patrones similares y nuevos intentos de conexión.
- Mantener los sistemas y aplicaciones parchados (especialmente servicios expuestos: RDP, VPN, correo).
- Ejecutar un escaneo completo de malware en los equipos internos para descartar compromisos vinculados a esta IP maliciosa.
- Revisar configuraciones de correo (SPF, DKIM, DMARC) para evitar abuso de infraestructura en spam.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Si algún equipo muestra indicios de comunicación activa con IP maliciosa, aislarlo de la red hasta validar que esté libre de malware.

Conclusión

El hallazgo refleja actividad persistente desde direcciones maliciosas hacia infraestructura del sector. Es fundamental aplicar bloqueos inmediatos y fortalecer la supervisión de eventos en el SIEM, a fin de reducir el riesgo de intrusión y compromiso de sistemas críticos.

Fuentes:

- https://www.abuseipdb.com/check/178.22.24.30?utm_source
- https://www.whois.com/whois/178.22.24.30
- https://www.virustotal.com/gui/ip-address/178.22.24.30
- https://otx.alienvault.com/indicator/ip/178.22.24.30
- https://www.shodan.io/host/178.22.24.30

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) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570