Alerta ID:	0048
Fecha del reporte:	20/10/2025
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:	Infraestructura tecnológica y servicios de red de entidades públicas
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 direcciones IP clasificadas 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 internas del sector, los cuales no fueron bloqueados y representan un riesgo de comunicación con infraestructura maliciosa.

Descripción del Incidente

Fuente de detección: SIEM sectorial.

Categoría: Tráfico permitido desde IPs maliciosas (IPSum).

Severidad: Alta.

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

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

Comportamiento observado: persistencia en intentos de conexión desde múltiples geolocalizaciones (Estados Unidos, China, Rusia, Reino Unido, entre otros).

Se anexa documento en formato Excel con las direcciones IP identificadas durante el análisis en el SIEM. Estos registros corresponden a eventos de tráfico permitido desde orígenes clasificados como maliciosos en listas negras (IPSum). La información se presenta de manera consolidada para servir como referencia en la gestión de riesgos y la implementación de medidas de mitigación.

Impacto Potencial

- Posible comunicación con servidores de C2.
- Riesgo de descarga o propagación de malware en equipos internos.
- Compromiso de información sensible de los sistemas expuestos.
- Afectación reputacional y operativa en caso de explotación exitosa.
- Posible Ataques de denegación de servicios (DDoS) a los servicios de la entidad.

Recomendaciones

- Bloquear inmediatamente las IPs maliciosas detectadas en firewalls y controles de red.
- **Configurar las IP como IoC** en las herramientas de seguridad para activar alertas y cortar la comunicación maliciosa.

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

- **Correlacionar en el SIEM** nuevos eventos relacionados a estas IP y generar notificaciones en tiempo real.

- Fortalecer políticas de filtrado perimetral, de forma que este tipo de tráfico no sea permitido sin análisis previo.

- Mantener monitoreo constante en busca de patrones similares y nuevos intentos de conexión.

- Validar conexiones inusuales hacia el exterior y **revisar logs históricos** de tráfico para descartar compromisos.

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.

En caso de que después de verificar las direcciones IP´s reportadas se detecte que algunas son direcciones IP´s permitidas por favor reportarlas al correo electrónico del CSIRT con el fin de que estas sean excluidas y así evitar que sean reportadas nuevamente por el SIEM.

Fuentes:

- Herramienta de monitoreo FortiSIEM CSIRTSALUD.

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

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

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