Alerta ID:	0031
Fecha del reporte:	17-09-2025
Entidad:	Todas las entidades del ecosistema digital
Título:	Observación de direcciones IP maliciosas reportadas en el Boletín Ciberinteligencia 172 dentro de eventos del SIEM
Herramienta de detección	Fortisiem
Activo involucrado:	Infraestructura tecnológica y servicios de red de entidades públicas
Tipo de alerta:	Correlación de eventos
Nivel de riesgo:	Alto

Objetivo:

Alertar a las entidades del ecosistema digital sobre la detección en el SIEM de eventos asociados a direcciones IP maliciosas previamente reportadas en el **Boletín Ciberinteligencia 172**, con el fin de reforzar acciones de monitoreo, mitigación y protección de infraestructuras críticas.

Descripción:

El **Boletín Ciberinteligencia No. 172 (16/09/2025)** reportó un conjunto de **direcciones IP maliciosas asociadas a malware y servidores de comando y control (C2)**. Posteriormente, se identificó que **algunas de estas IP's han sido observadas en eventos del SIEM**, afectando a varias entidades del ecosistema digital.

Se pretende que **cada entidad integre estas direcciones IP como IoC en sus sistemas de seguridad y control perimetral**, a fin de **bloquear conexiones maliciosas** y prevenir un posible compromiso de la infraestructura tecnológica.

Direcciones IP reportadas (Boletín 172):

Asociadas a Malware

- 151.101.194.133 – Estados Unidos
- 8.250.243.254 – Estados Unidos
- 91.198.174.192 – Estados Unidos
- 148.135.111.20 – Suecia
- 152.32.245.27 – Tailandia
- 162.142.125.124 – Estados Unidos
- 162.142.125.44 – Estados Unidos
- 162.142.125.119 – Estados Unidos
- 192.171.62.226 – Canadá

Asociadas a Servidores C2 (Command & Control)

- 139.99.125.38 – Singapur

- 94.130.164.163 – Alemania
- 46.28.68.134 – Ucrania
- 131.153.56.98 – Chicago (EE. UU.)
- 104.140.244.186 – Estados Unidos
- 178.128.242.134 – Ámsterdam
- 192.110.160.114 – Estados Unidos
- 45.9.148.36 – Ámsterdam
- 144.217.14.139 – Canadá

Recursos y versiones afectadas:

- Infraestructura de red, servidores y estaciones de trabajo conectadas a internet en entidades del ecosistema digital.
- No se limita a un sistema operativo específico.

Vector de impacto:

Conexiones a direcciones IP asociadas a **malware y C2**, que pueden derivar en robo de información, persistencia en los sistemas comprometidos y movimientos laterales dentro de las redes institucionales.

Recomendaciones de mitigación:

- **Bloquear inmediatamente** en firewalls, IDS/IPS, proxys y listas negras las direcciones IP reportadas en el Boletín 172.
- **Configurar las IP como IoC** en las herramientas de seguridad para activar alertas y cortar la comunicación maliciosa.
- **Correlacionar en el SIEM** nuevos eventos relacionados a estas IP y generar notificaciones en tiempo real.
- **Aplicar inteligencia de amenazas (Threat Intel)** en la gestión de incidentes.
- **Reforzar la autenticación multifactor (MFA)** en accesos a sistemas críticos y servicios en la nube.
- **Actualizar software y sistemas** con los últimos parches de seguridad.
- Validar conexiones inusuales hacia el exterior y **revisar logs históricos** de tráfico para descartar compromisos.

Fuentes:

- Boletín Ciberinteligencia N.º 172 – CCOCI (16-09-2025)

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) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.