| | |
|---|---|
| **Alerta ID:** | 0030 |
| **Fecha del reporte:** | 17-09-2025 |
| **Entidad:** | Todas las entidades del ecosistema digital |
| **Título:** | Observación de direcciones IP maliciosas reportadas en el Boletín Ciberinteligencia 171 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 171**, con el fin de reforzar acciones de monitoreo, mitigación y protección de infraestructuras críticas.

## Descripción:

El **Boletín Ciberinteligencia No. 171 (15/09/2025)** 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 se han visto activamente en eventos del SIEM**, afectando a múltiples entidades del ecosistema digital.

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

**Direcciones IP reportadas (Boletín 171):**

**Asociadas a Malware**

- 87.236.176.95 – Bélgica
- 185.196.220.81 – Estados Unidos
- 162.142.125.216 – Estados Unidos
- 205.210.31.192 – Canadá
- 172.104.11.4 – Estados Unidos
- 64.62.197.116 – Estados Unidos
- 205.210.31.48 – Canadá
- 185.93.89.118 – Inglaterra
- 87.236.176.101 – Bélgica

**Asociadas a Servidores C2 (Command & Control)**

- 185.215.113.84 – Seychelles
- 194.58.112.174 – Rusia
- 64.70.19.203 – Estados Unidos
- 45.61.165.8 – Estados Unidos
- 172.86.89.51 – Francia
- 172.67.133.185 – Estados Unidos
- 185.222.57.76 – Ámsterdam
- 222.186.134.85 – China
- 66.97.45.219 – Argentina

## 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 171.
- **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 171 – CCOCI (15-09-2025)

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.