Alerta ID:	0035
Fecha del reporte:	01/10/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Indicadores de compromiso (IOC) - Direcciones IP públicas 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 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 IP públicas del sector, que no fueron bloqueadas y por lo tanto 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.

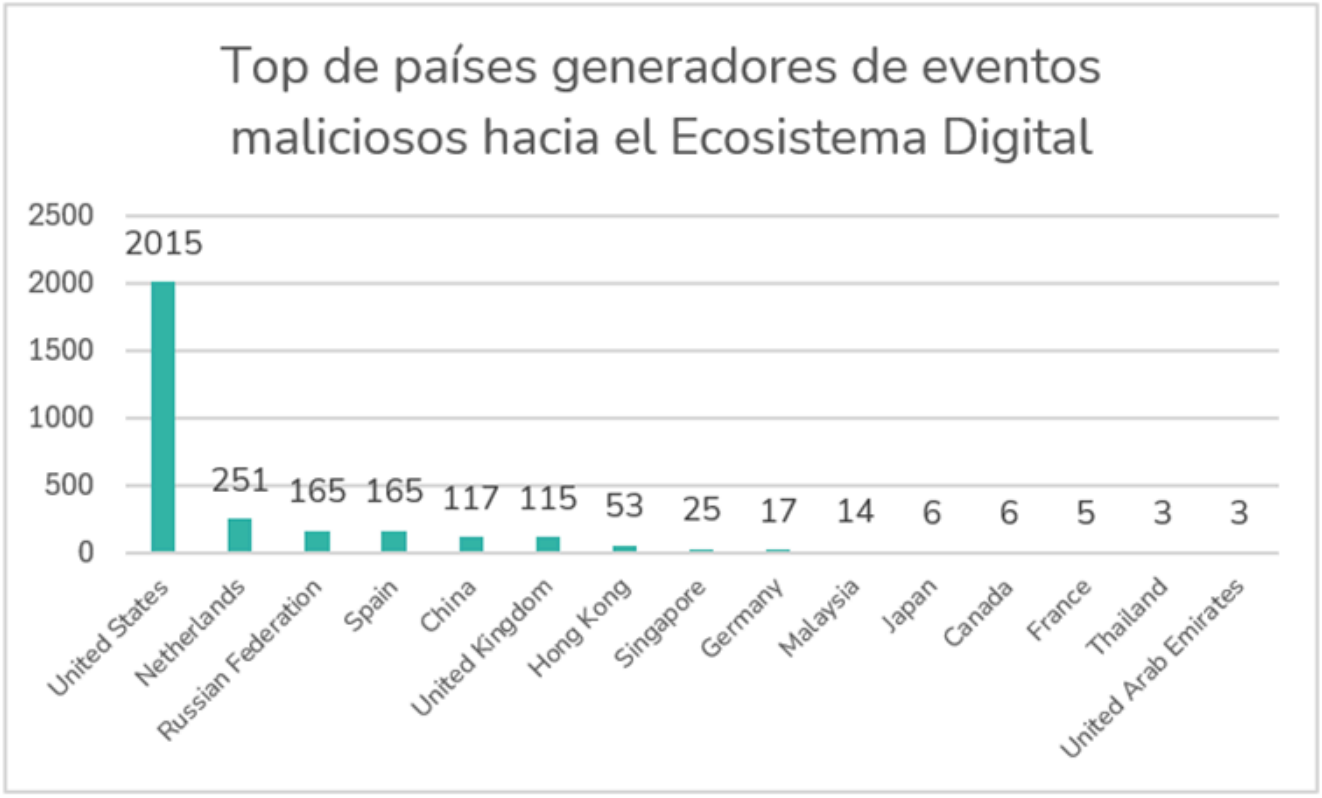
CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

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).

A continuación, se relaciona el Top 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.

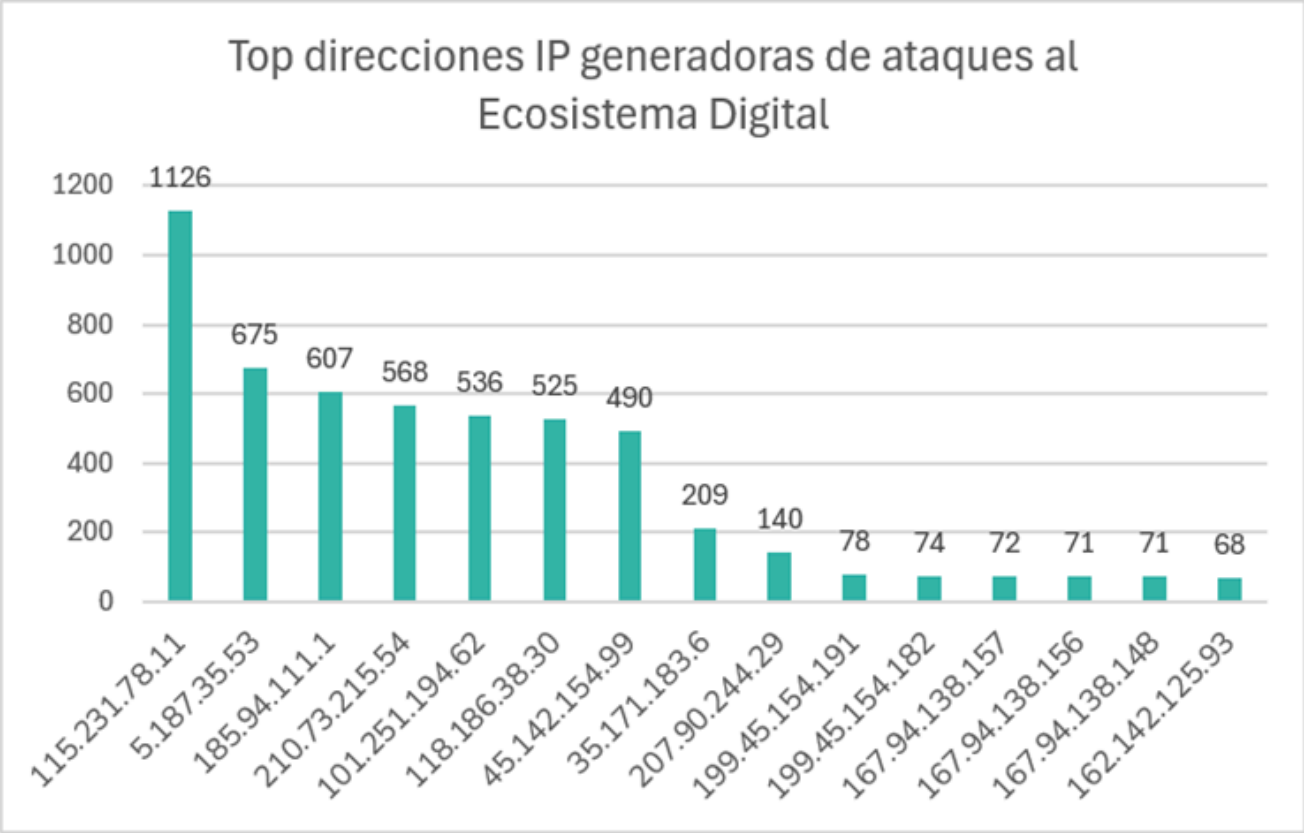
Ilustración 1. Top países generadores de eventos maliciosos



Fuente: elaboración propia con eventos del SIEM Sectorial

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

Ilustración 2. Top direcciones IP generadoras de ataques al ecosistema Digital



Fuente: elaboración propia con eventos del SIEM Sectorial

Plataformas donde están reportadas las IPs con mayor número de ataques

Source IP	Plataforma	Url
204.76.203.212	VirusTotal	https://www.virustotal.com/gui/ip-address/204.76.203.212
45.135.193.100	AbuseIPDB	https://www.abuseipdb.com/check/45.135.193.100
204.76.203.206	VirusTotal	https://www.virustotal.com/gui/ip-address/204.76.203.206

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

Source IP	Plataforma	Url
115.231.78.11	AbuseIPDB	https://www.abuseipdb.com/check/115.231.78.11
5.187.35.53	IPinfo	https://ipinfo.io/5.187.35.53
204.76.203.219	AbuseIPDB	https://www.abuseipdb.com/check/204.76.203.219
185.94.111.1	AbuseIPDB	https://www.abuseipdb.com/check/185.94.111.1
210.73.215.54	VirusTotal	https://www.virustotal.com/gui/ip-address/210.73.215.54
118.186.38.30	AbuseIPDB	https://www.abuseipdb.com/check/118.186.38.30
45.142.154.99	AbuseIPDB	https://www.abuseipdb.com/check/45.142.154.99
93.174.93.12	AbuseIPDB	https://www.abuseipdb.com/check/93.174.93.12

Impacto Potencial

- Compromiso de seguridad de la red ya que estas IPs 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 muchas de esas IPs están documentadas por hacer port scanning, fuerza bruta en RDP/SSH/HTTP, si algún equipo responde podría estar exponiendo servicios mal configurados o credenciales débiles.

- 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

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

listas negras lo que podría ocasionar emails rebotados o bloqueados.

Recomendaciones

- Bloquear inmediatamente las IPs maliciosas detectadas en firewalls y controles de red. La totalidad de las IPs maliciosas se encuentran en el Anexo 1. Direcciones IP generadoras de eventos maliciosos (IoC).xlsx
- Revisar los equipos que hayan sido destino de las conexiones para descartar compromiso. De igual forma, verificar que los Endpoints internos no se encuentren generando tráfico a estas direcciones IP.
- 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.
- Mantener los sistemas y aplicaciones parcheados (especialmente servicios expuestos: RDP, VPN, correo).
- Ejecutar un escaneo completo de malware en los equipos internos para descartar compromisos vinculados a las IPs maliciosas detectadas
- Revisar configuraciones de correo (SPF, DKIM, DMARC) para evitar abuso de infraestructura en spam.
- Si algún equipo muestra indicios de comunicación activa con IP maliciosa, aislarlo de la red hasta validar que esté limpio.

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

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://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-54910
- https://cybersecuritynews.com/critical-microsoft-office-vulnerabilities/?utm_source

Anexo:

- Anexo 1. Direcciones IP generadoras de eventos maliciosos (IoC)

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