

Ciberseguridad Regional, la importancia de la colaboración regional

III Foro Regional sobre Interconectividad, Ciberseguridad e IPv6

Fred L. Clark, M. Sc

Superintendencia de Telecomunicaciones, Guatemala

Definición de Ciberseguridad

- La **ciberseguridad** es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.
- Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno.
- Resolución 181, Recomendación ITU-T X.1205

Ciberseguridad*

Los principios de seguridad incluyen una o más de las siguientes:

- disponibilidad;
- integridad, que puede incluir la autenticidad y el no repudio;
- confidencialidad.

- Convención de Budapest sobre el Cibercrimen

Antecedentes

- En el año 2002, 30 países miembros de la OEA firmaron la Convención Interamericana contra el Terrorismo [AG/RES. 1840](#).
- Desde Belice hasta Panamá, todos los Estados de Centroamérica la firmaron, incluso la República Dominicana.
- En el 2006 varios países de Centroamérica recibieron capacitación de primer orden patrocinada por CICTE.
- En el 2008 Guatemala organizó, con el apoyo de CICTE, un taller internacional sobre cómo establecer un CSIRT.
- Asistieron delegaciones de Centroamérica y de todo el continente.
- El taller contó con instructores de Argentina, Brasil, EE UU, y Uruguay

Antecedentes

- Cuatro años más tarde, en el 2012, Guatemala nuevamente organizó otro taller con presencia de toda América.
- Asistieron delegados de países de Centroamérica, el Caribe y Suramérica.
- Se contó nuevamente con el apoyo de CICTE y CERT/CC del SEI de la Universidad Carnegie-Mellon, en Pittsburgh, PA.
- CICTE ha apoyado en distintas ocasiones, talleres de simulación de situaciones para evaluar el riesgo en distintos países de Centroamérica.

Otra iniciativa

- Adicionalmente a los esfuerzos del CICTE de la OEA, existe otra iniciativa de LACNIC llamada Proyecto Amparo.
- Amparo inició como un proyecto orientado a hacia el fortalecimiento, difusión y conocimiento de los CSIRT.
- A partir del 2013 se ha dedicado a capacitar y fortalecer a los miembros de los equipos de CSIRT en temas como:
 - Seguridad en DNS / Despliegue de DNSSEC
 - Enrutamiento seguro (mejores prácticas, certificación de recursos, uso de RPKI)
 - Seguridad en redes
 - Consecuencias del agotamiento de IPv4 en la seguridad de Internet y en particular en la gestión de incidentes

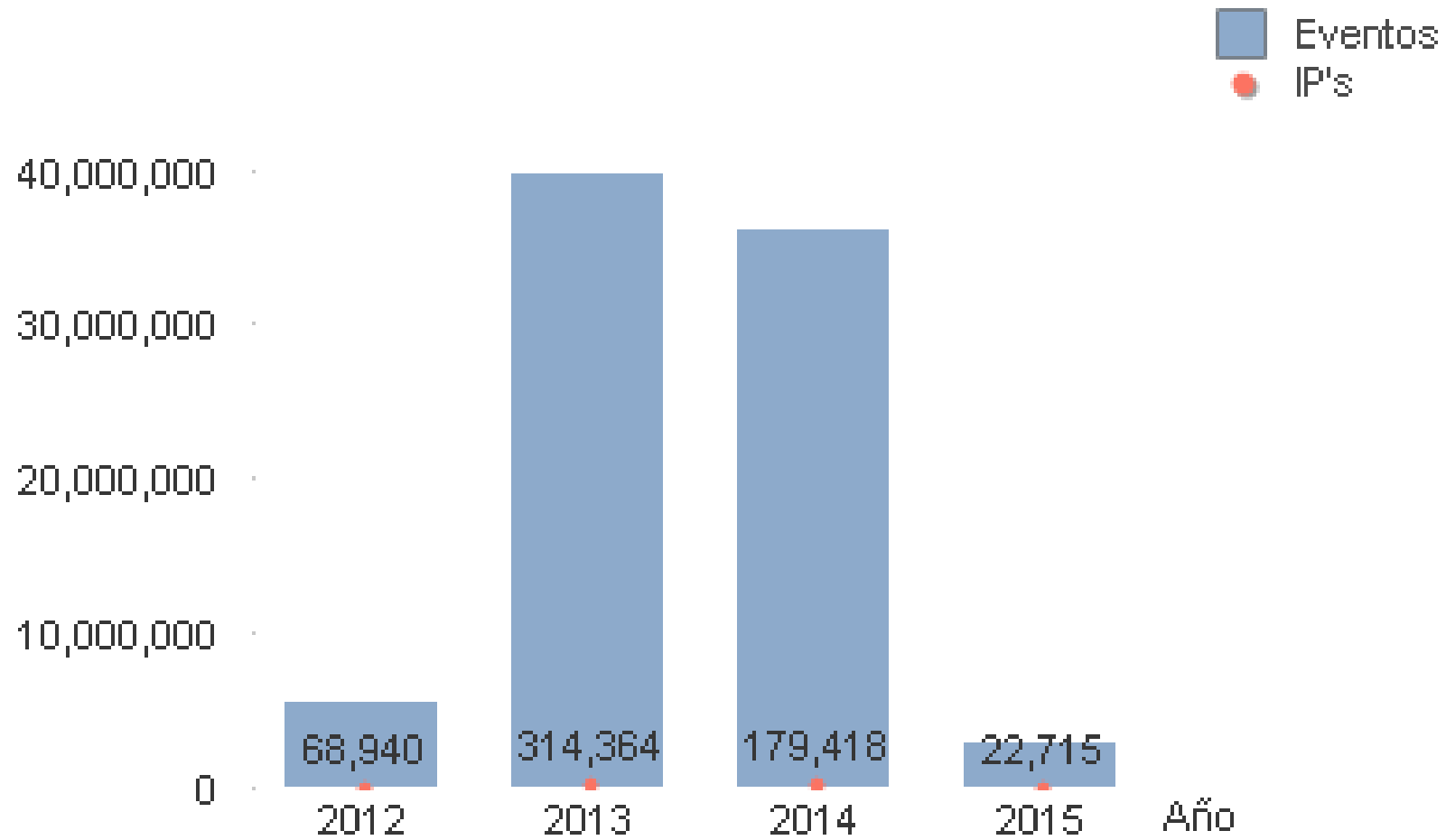
Talleres regionales de Amparo

- Ha organizado Talleres y encuentros desde el 2010:
- Seis en el 2010, uno de los cuales fue en República Dominicana;
- Cinco en el 2011, uno en Panamá y 1 en Liberia, Costa Rica;
- Tres en el 2012;
- Uno en el 2013;
- Uno en Honduras en el 2014;
- Tres en lo que va del 2015, uno de los cuales fue en Costa Rica.

¿Está Centroamérica libre de ataques?

- Cuantos de ustedes creen que Centroamérica y República Dominicana están libres de incidentes de Ciberseguridad?

Eventos



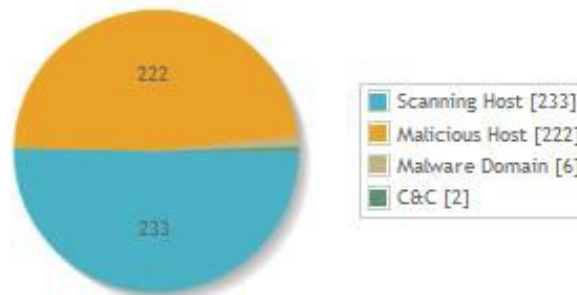
Clasificación de la Actividad maliciosa hacia Guatemala



General statistics

Number of IPs in the database 315
 Latest update 2015-02-26 16:15:23

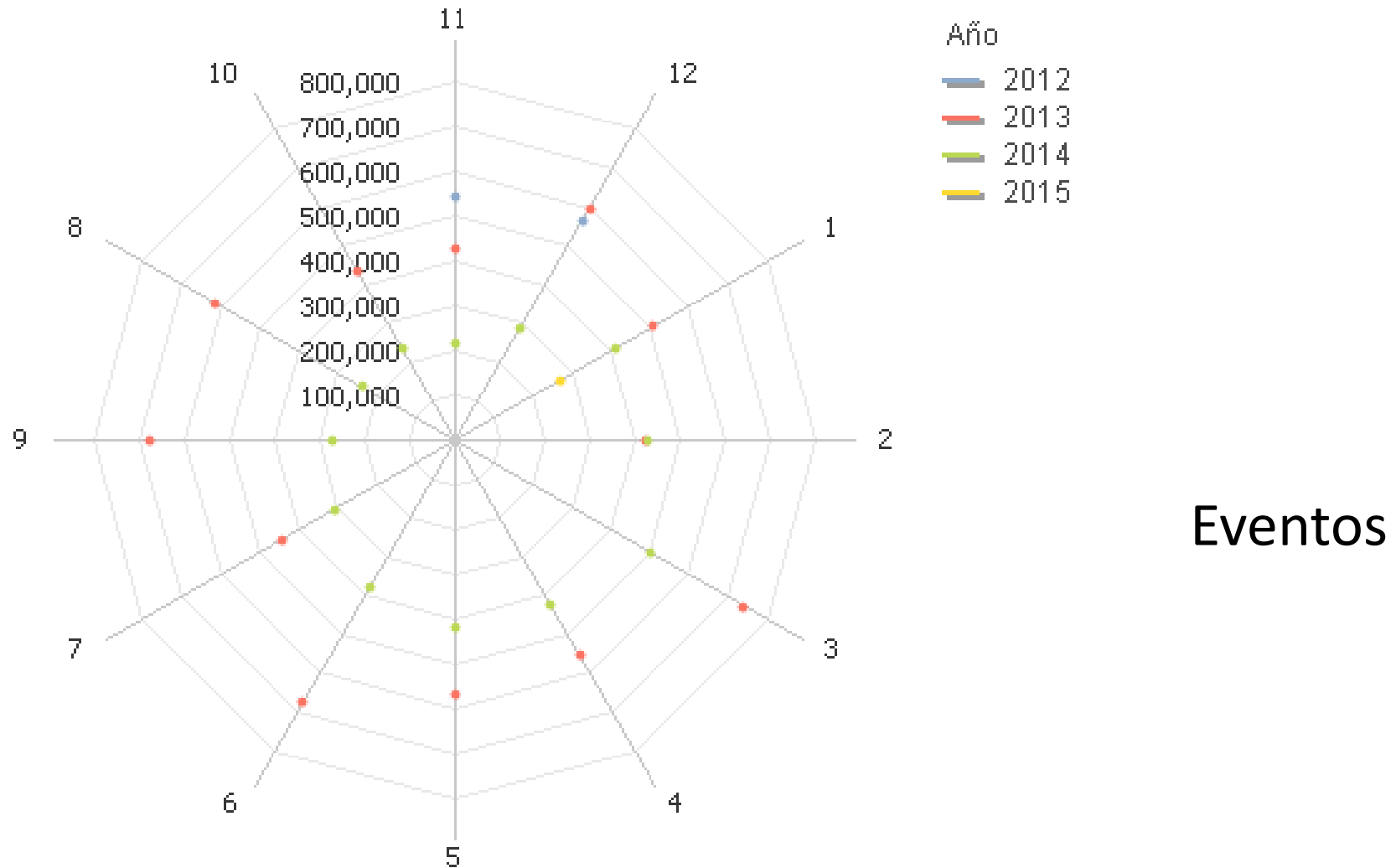
Malicious IPs by Activity



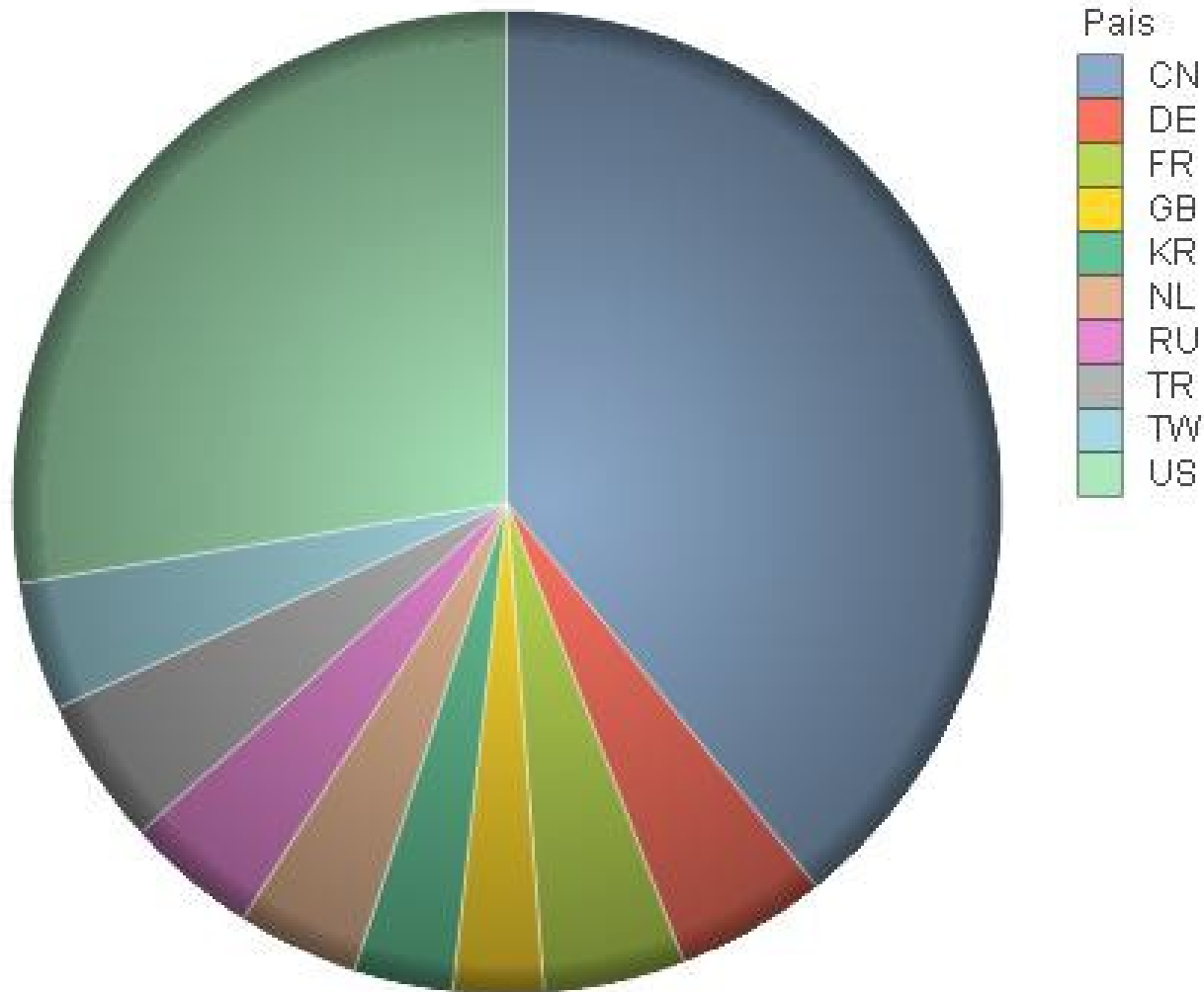
Top 10 Countries

Country	IPs #
China	132
France	37
United States	33
Germany	17
Netherlands	8
South Korea	6
Russian Federation	6
United Kingdom	6
India	3
Viet Nam	2

Actividad hacia Centroamérica oct 2012/ene 2015

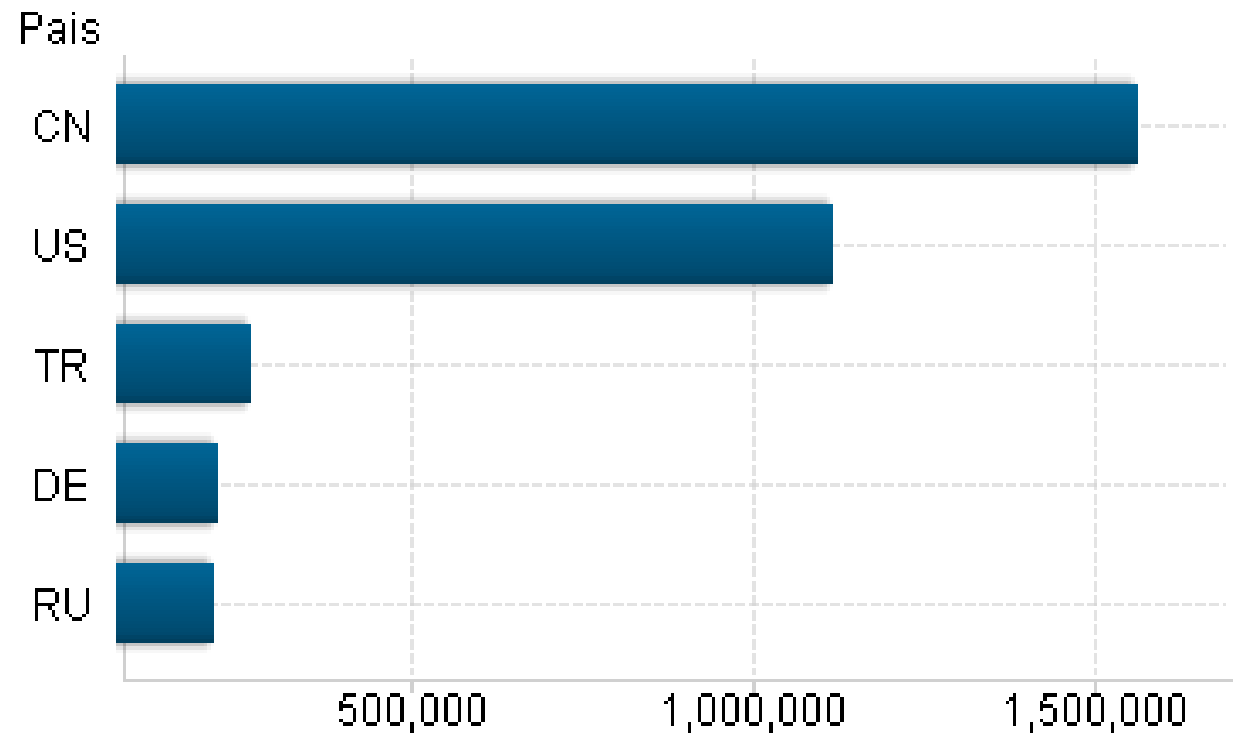
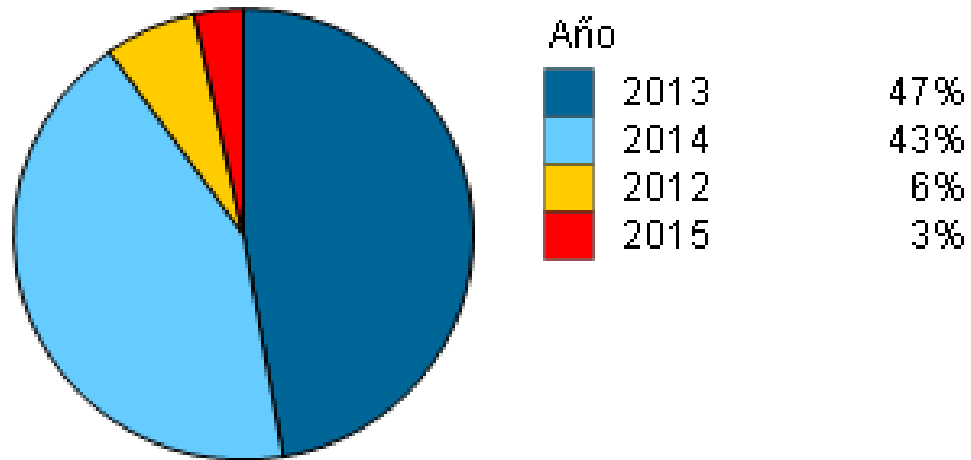


Actividad hacia Centroamérica oct 2012/ene 2015

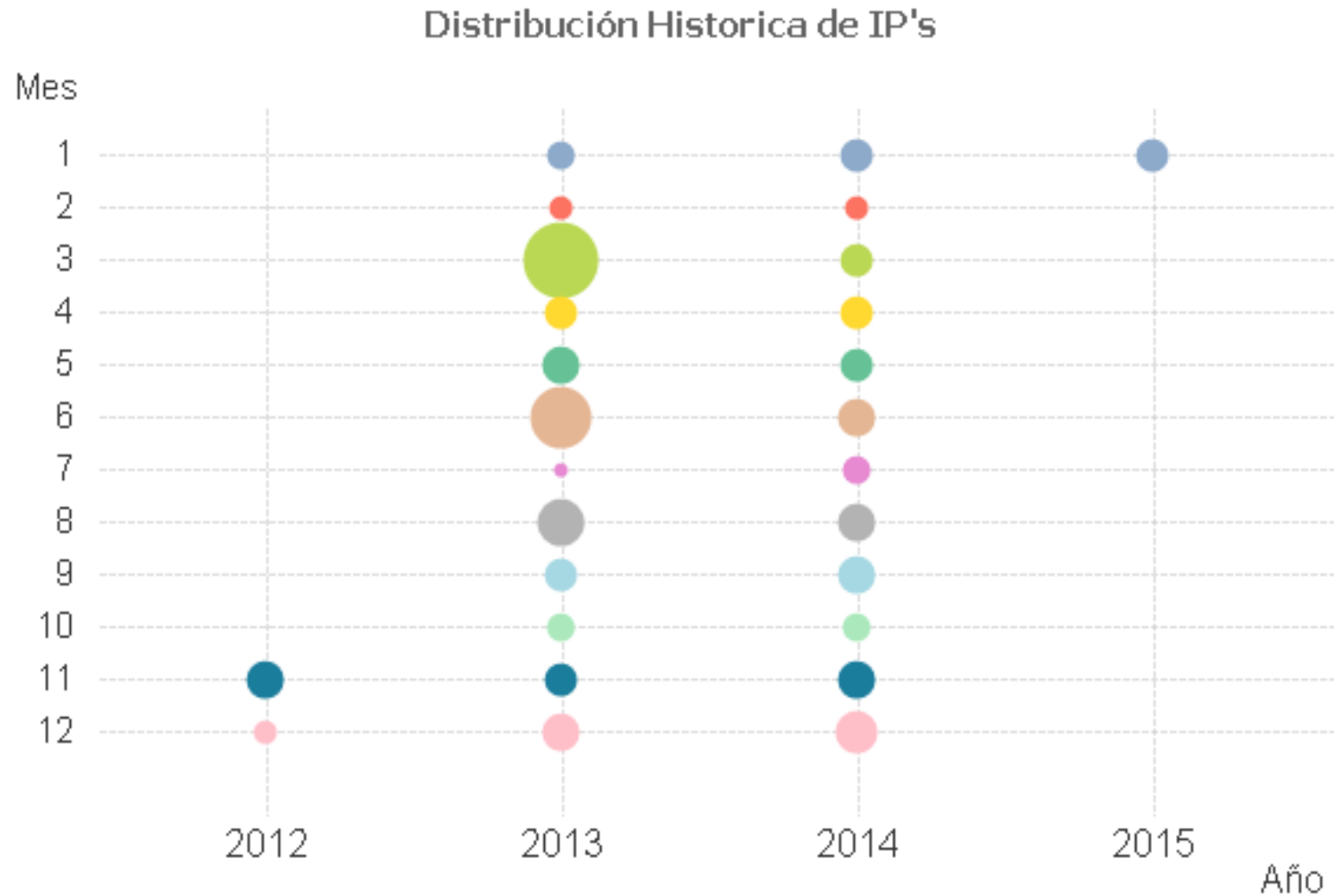


País de origen de la actividad maliciosa, top 10.

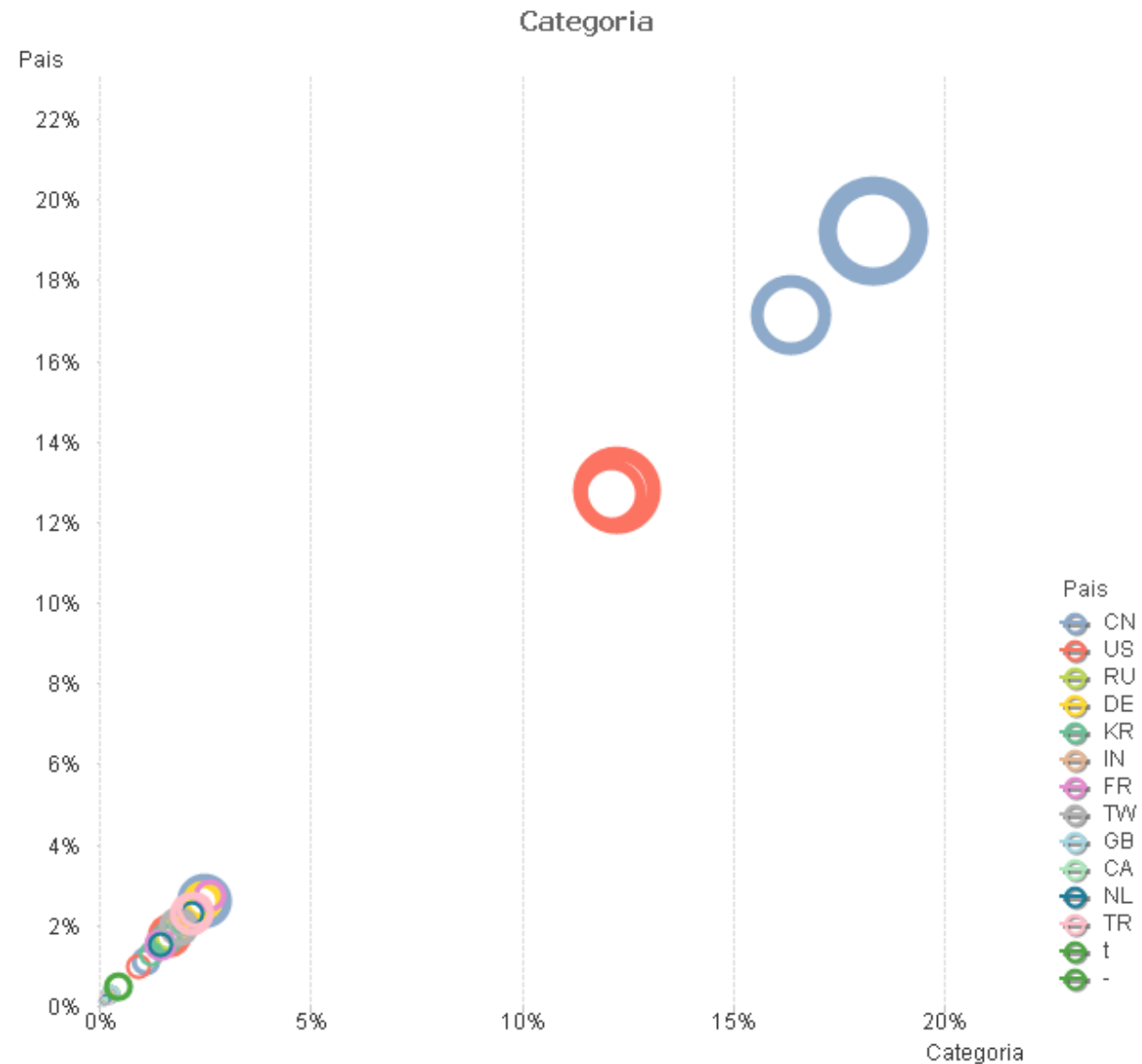
Hacia Centroamérica, IPs vrs eventos diarios



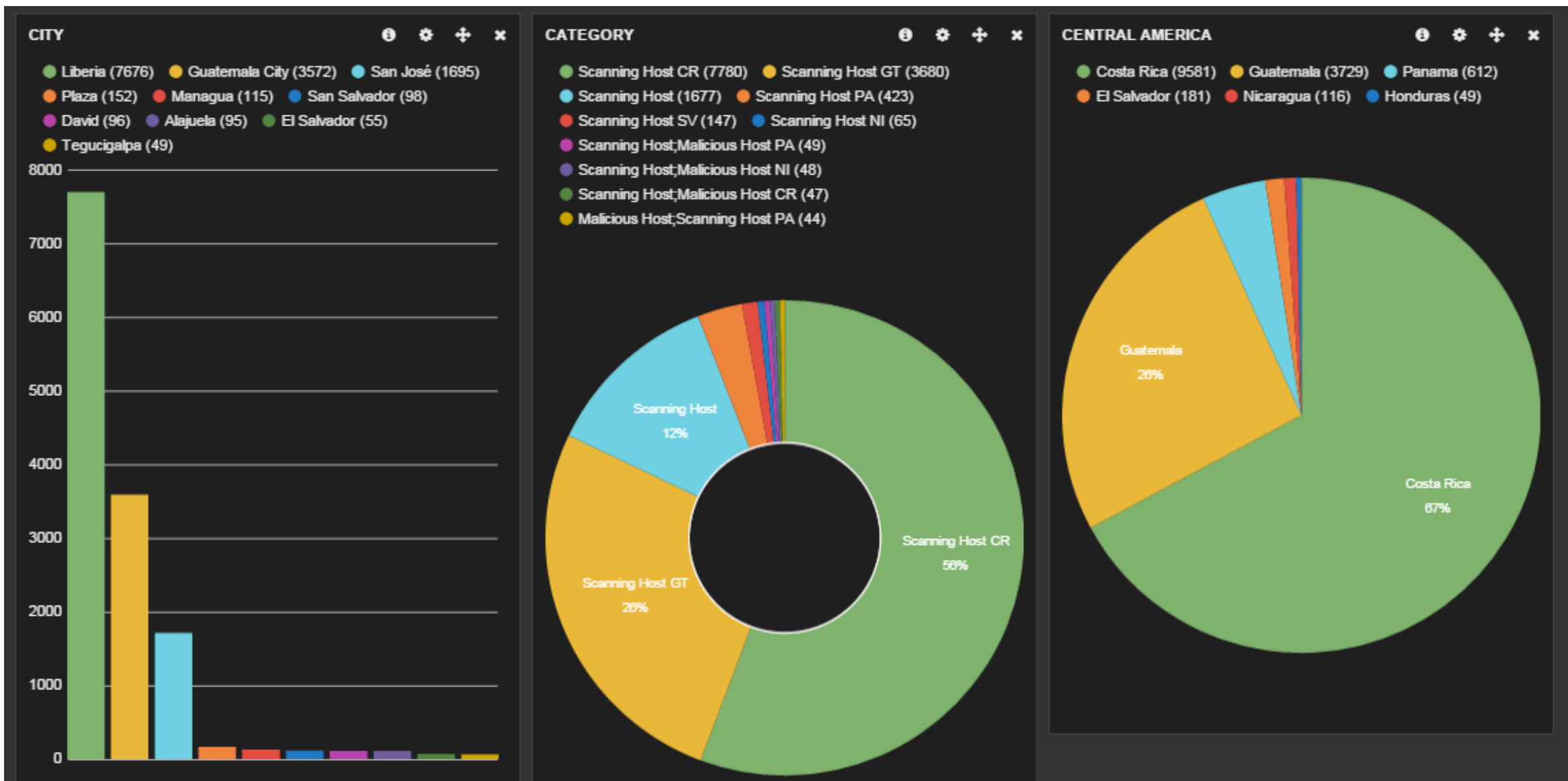
Hacia Centroamérica, por dirección IP



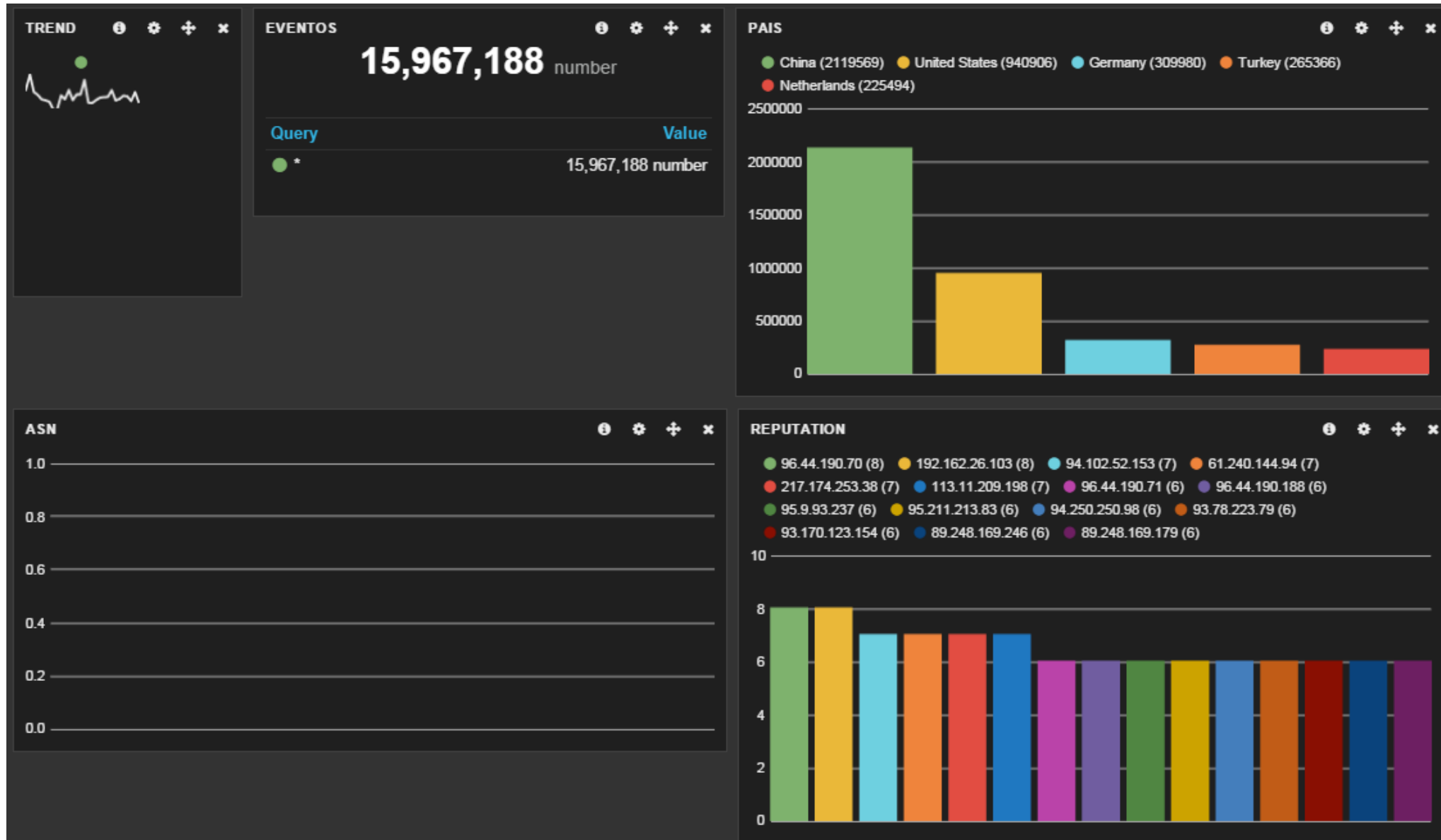
Hacia Centroamérica, por país



Resultado del análisis del tráfico



Análisis: origen de los ataques a Centroamérica



Ataques originados desde Centroamérica

- 1. Guatemala (2 casos de phishing)
- 2. Guatemala (2 ddos involucrados desde Guatemala)
- 3. Salvador robo de intidad digital
- 4. Infeccion de Spyware en Nicaragua

Comentarios

- Después de ver estas láminas podemos concluir que Centroamérica, (sin incluir la República Dominicana); si está vulnerable a los ataques maliciosos de personas en todo el mundo.
- Entonces, ¿Porque es importante buscar la colaboración regional a través de Organizaciones Internacionales?



Comentarios

- Después de ver estas láminas podemos concluir que Centroamérica, sin incluir la República Dominicana; si está vulnerable a los ataques maliciosos de personas en todo el mundo.
- Entonces, ¿Porque es importante buscar la colaboración regional a través de Organizaciones Internacionales? Tomar en consideración:
 - Falta de Equipos Nacionales de Respuesta a Incidentes de Seguridad Cibernética;
 - Falta de Legislación especializada que permita perseguir y castigar a personas que llevan a cabo los ataques;
 - Falta de clasificación de la infraestructura crítica y protección de la misma.