Telefónica

REPORTE DE TENDENCIAS_

Detección de botnets en Twitter durante eventos deportivos

En colaboración de:

etisalat | Singtel

Índice

1. Resumen ejecutivo

Este informe es un análisis de las **redes sociales de bots**. Hemos analizado dos grandes conversaciones de Twitter e identificado el comportamiento de varios grupos de perfiles con actividades automáticas y no estándar. La primera conversación se centra en la **Copa Mundial de la FIFA 2018**, celebrada entre el 14 de junio y el 15 de julio. Hemos trabajado en las comunidades de toda la conversación y descubrimos varios grupos de perfiles que se comportaban de forma extraña. Después de aplicar algoritmos propietarios, confirmamos que esas comunidades eran **botnets de difusión de contenidos** que fueron activadas durante los partidos de fútbol para compartir **URLs ilegales de streaming**.

Con el fin de hacer un análisis más amplio, hemos investigado un mayor número de deportes en todo el mundo durante cinco semanas: desde el 1 de noviembre hasta el 10 de diciembre. Esta nueva conversación cubrió el tema del **streaming deportivo en Twitter** e incluyó importantes eventos como la Premier League, la UEFA Champions League o los partidos semanales de la NFL en Estados Unidos. No sólo descubrimos que algunas de las botnets identificadas en la Copa Mundial de la FIFA seguían activas y difundiendo contenido actual, sino que también se encontraron **nuevas botnets** centradas en diferentes deportes.

Los objetivos de este informe son:

- Encontrar botnets relacionadas con la difusión ilegal de eventos deportivos.
- Observar su evolución a lo largo del tiempo.
- Identificar nuevas botnets a raíz de las que ya habíamos encontrado.
- Entender el comportamiento de una botnet en Twitter.
- Prevenir y controlar la difusión de contenido a partir de botnets en Twitter.

Como resultado, hemos aprendido a identificar este tipo de redes, y hemos comenzado a aplicar estos conocimientos en varios casos de uso, como en **crisis de reputación**.

Al comparar las dos conversaciones analizadas, hemos podido observar que **25 perfiles de bots** coinciden y han estado activos y compartiendo contenido de streaming desde junio de 2018.

Estas han sido algunas de las conclusiones:

- Las botnets de Twitter no suelen estar asociadas a un único deporte; usan cualquier evento deportivo de relevancia para difundir el contenido de forma ilegal.
- Los tweets que difunden contenido ilegal relacionado con el fútbol americano representan el 0,5% sobre el total de los tweets de este deporte.
- La mayor parte de países solo tiene un número reducido de servidores que difunden contenido ilegal.
- Los tres países que más contenido ilegal difunden son Estados Unidos, España y Alemania.

2. Contexto

Es bien sabido que la industria de la radiodifusión y los derechos de los medios de comunicación en el deporte[1] está preocupada por la difusión ilegal, que afecta directamente a sus ingresos previstos. Los métodos más conocidos son **a través de sistemas de satélite extranjeros** (alguien que intenta vender un sistema de satélite extranjero) o a través de **páginas web no autorizadas**.

Por ejemplo, la Premier League del Reino Unido tiene una página web para informar sobre estos casos https://www.idinquiries.com/premier-league. en España también existe una organización llamada IPRORED que ofrece protección de los derechos en Internet (http://www.iproded.com/english/index.html). Además, LaLiga ha desarrollado su propia tecnología para enfrentarse a las emisiones ilegales.[2]

Primer análisis de conversación: Durante la última Copa Mundial de Fútbol de la FIFA 2018 celebrada en Rusia, observamos cómo diferentes botnets de Twitter difundieron ilegalmente los 64 partidos jugados gracias a los **tweets que compartían las URLs** a las que conectarse.

Segundo análisis de conversación: Hemos ampliado esta observación a más acontecimientos deportivos y a más países. Esta vez nos hemos centrado en otros deportes principales como el rugby, el cricket, el béisbol, el baloncesto y, por supuesto, el fútbol.

2.1. ¿Qué es una botnet?

Una **botnet** es un número de dispositivos conectados a Internet, cada uno de los cuales está ejecutando uno o más bots. Las botnets pueden utilizarse para realizar ataques de denegación de servicio distribuidos (ataques DDoS), robar datos, enviar spam y permitir al atacante acceder al dispositivo y a su conexión. El propietario puede controlar la botnet mediante el software de comando y control (C&C).

Muchos usuarios de Twitter son bots, que son cuentas controladas y a veces creadas por ordenadores. Los **bots de Twitter** pueden enviar tweets de spam, manipular la opinión pública, ser utilizados para el fraude en línea y, en este caso, para **promover el acceso por URL a contenidos deportivos ilegales**. Una botnet contiene un único tipo de bot, que muestra exactamente las mismas propiedades en toda la botnet. Los bots se venden por dinero y se venden como falsos seguidores.

[1] https://www.wipo.int/ip-sport/en/broadcasting.html

[2] https://elpais.com/deportes/2018/10/30/es_laliga/1540911095_179420.html

Hay botnets en Twitter para muchos casos, como por ejemplo para promover comportamientos antipolíticos, secuestro de cuentas relacionadas con criptomonedas[3], etc. Una de las mayores botnets de Twitter tenía 350.000 cuentas.[4]

3. Metodología: Aldara

Aldara es una herramienta de desarrollo propio para realizar Análisis de Redes Sociales. Aplica diferentes algoritmos propietarios y Machine Learning con el fin de proporcionar los conocimientos que los analistas requieren.

Aldara trabaja en varias fases:

1. **Agregación de fuentes de datos**: Conectado directamente a Twitter y está integrado con otros socios para proporcionar acceso a diferentes fuentes de datos.

2. **Aplicación de Inteligencia Artificial y Machine Learning**: Usando Machine Learning y Procesamiento del Lenguaje Natural para procesar información en tiempo real y por lotes. Además, Aldara utiliza técnicas patentadas para comprender mejor cómo interactúan las personas.

3. **Empoderación de la empresa**: Proporciona cuadros de mando e integraciones con herramientas empresariales de terceros para ayudar a los analistas a comprender mejor lo que está ocurriendo realmente en las redes sociales.

4. **Proporcionamiento de Inteligencia Accionable**: el cerebro de Aldara tiene la capacidad de proporcionar percepciones relevantes desde el principio, proporcionando percepciones que ayudan a contextualizar los perfiles sociales y las conversaciones.

Como resultado, Aldara es utilizado por los analistas para afrontar retos como:

- **Contextualización de perfiles**: contextualizar perfiles anónimos y permitir identificar los grupos a los que pertenecen e incluso quiénes son en la vida real.
- **Análisis profundo de la conversación**: comprender mejor cómo interactúan las personas y separar el núcleo de la conversación real del ruido resiliente.
- **Identificación y análisis de influencers**: descubrimiento de nuevos influencers por tema y evaluación de los conocidos.
- **Estudios de mercado**: analizando qué están haciendo los competidores, cuáles son los mercados más relevantes y cuáles son los actores más importantes en todos ellos.
- **Evaluación de riesgos**: identificar los grupos y actores detrás de una campaña y analizar su comportamiento pasado para evaluar el riesgo real de un posible ataque.
- **Identificación de bots**: detección de campañas de desinformación lideradas por el bot contra su marca.

[3] https://nulltx.com/twitter-botnet-is-responsible-for-the-hijacking-of-cryptocurrency-related-accounts/

[4] https://www.newscientist.com/article/2117811-army-of-350000-star-wars-bots-found-lurking-on-twitter/

4. Primer analis de conversación: la Copa Mundial de Rusia 2018

Durante la Copa Mundial de la FIFA 2018 (14 de junio - 15 de julio) monitorizamos la conversación online en Twitter para identificar difusores de contenido ilegal. Para ello, combinamos varios componentes en la consulta para obtener los resultados más claros y formar un gráfico intuitivo. La consulta se construyó en inglés y contenía una combinación de términos relacionados con la Copa Mundial y la difusión de contenidos.

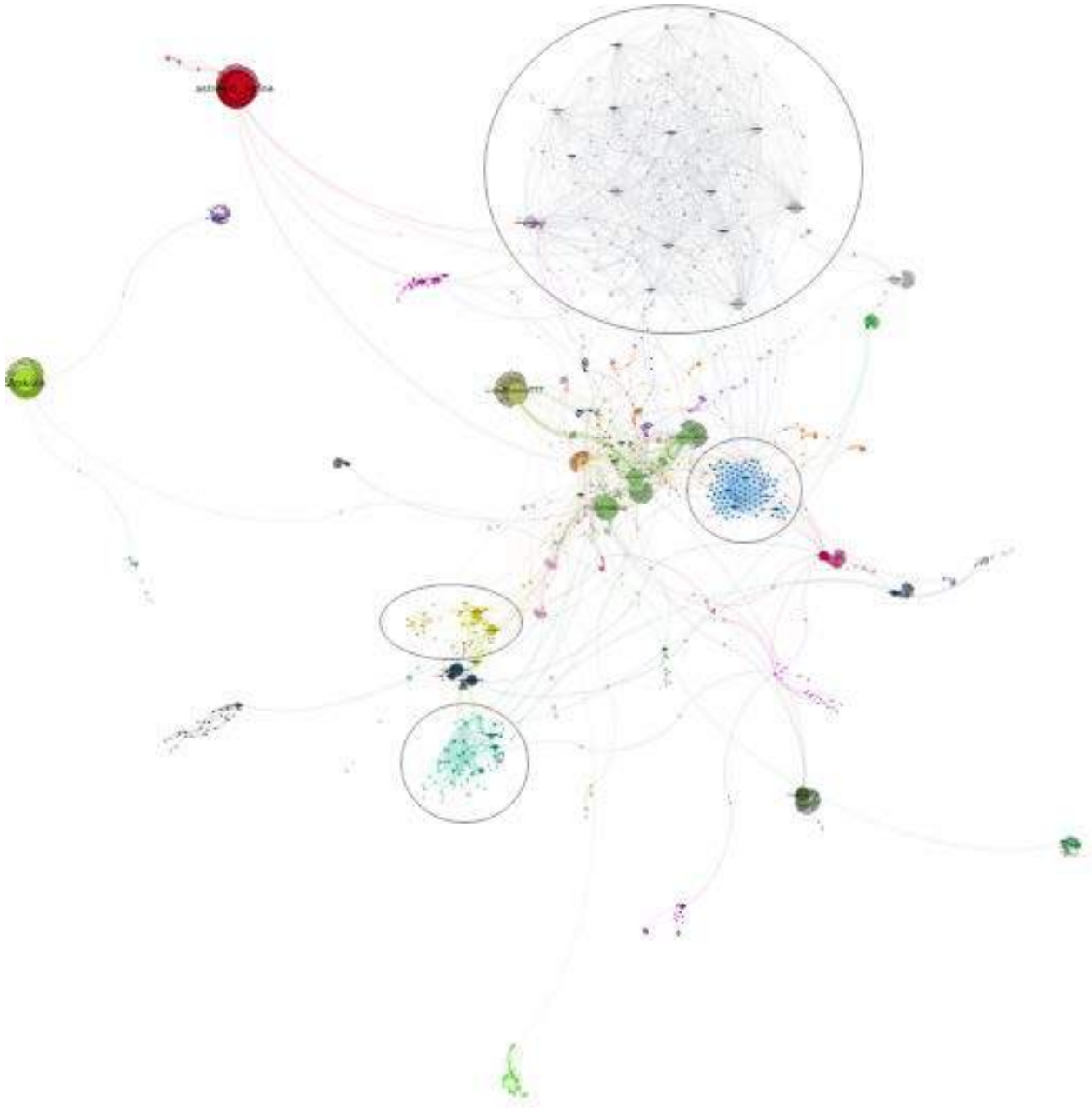
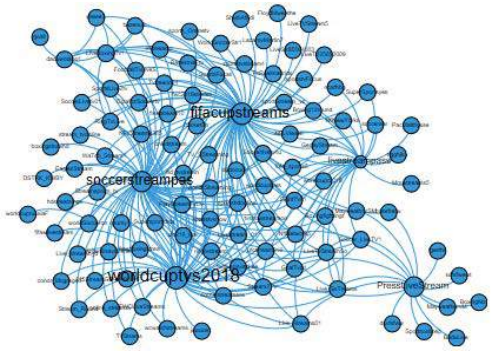
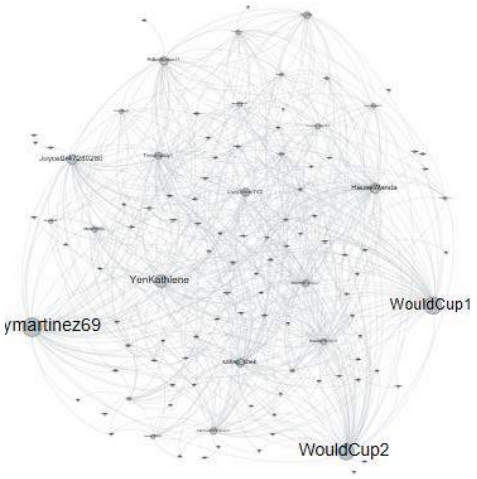


Figura 1: Conversación de Twitter sobre la retransmisión de partidos de fútbol

En el grafo podemos distinguir hasta 4 botnets:

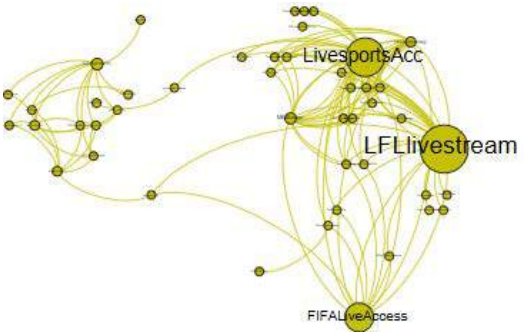


Botnet 1: Engloba el fútbol europeo. Esta botnet está formada por 106 perfiles, de los cuales 102 siguen activos.



Botnet 2: Engloba la mayoría de las ligas europeas. De las 111 cuentas iniciales, 2 han sido eliminadas o suspendidas.

Botnet 3: Engloba la NFL, AFL, UK (Premier) y el boxeo. Estaba formada por 67 perfiles, de los cuales 59 siguen activos.



Botnet 4: Engloba el boxeo, NFL y MLB. Estaba formada por 46 perfiles, de los cuales 44 siguen activos.

Figura 2: Botnets de Twitter

La forma de identificar estas botnets es **analizando el comportamiento comunicativo de los perfiles**. Como se puede ver en los ejemplos, las cuentas de cada botnet están todas interconectadas, mientras que, en una conversación normal, hay perfiles dominantes con muchas cuentas que difunden o que interactúan, como en la siguiente figura.

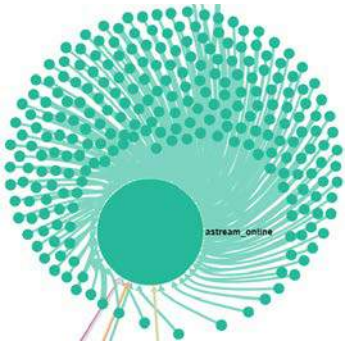


Figura 3: Conversación normal de Twitter

A partir del análisis de este grafo, hemos podido identificar el alcance del número de deportes de estas botnets (aparte de la Copa Mundial de Rusia) y hemos comprobado si siguen activas o han sido borradas o suspendidas en Twitter.

A partir de este análisis decidimos ir más allá en el análisis de las botnets difusoras de contenido y desarrollamos una metodología para identificar nuevas botnets en todo el mundo relacionadas con un espectro más amplio de deportes.

5. Segundo análisis de conversación: eventos deportivos en el mundo

Tras este primer análisis, decidimos ampliar el espectro de investigación y hemos investigado un mayor número de países y deportes como el rugby, el cricket, el futbol americano, el beisbol, el baloncesto y, de nuevo, el futbol.

Hemos monitorizado en Aldara todos los contenidos relacionados con el streaming de eventos deportivos durante 5 semanas.

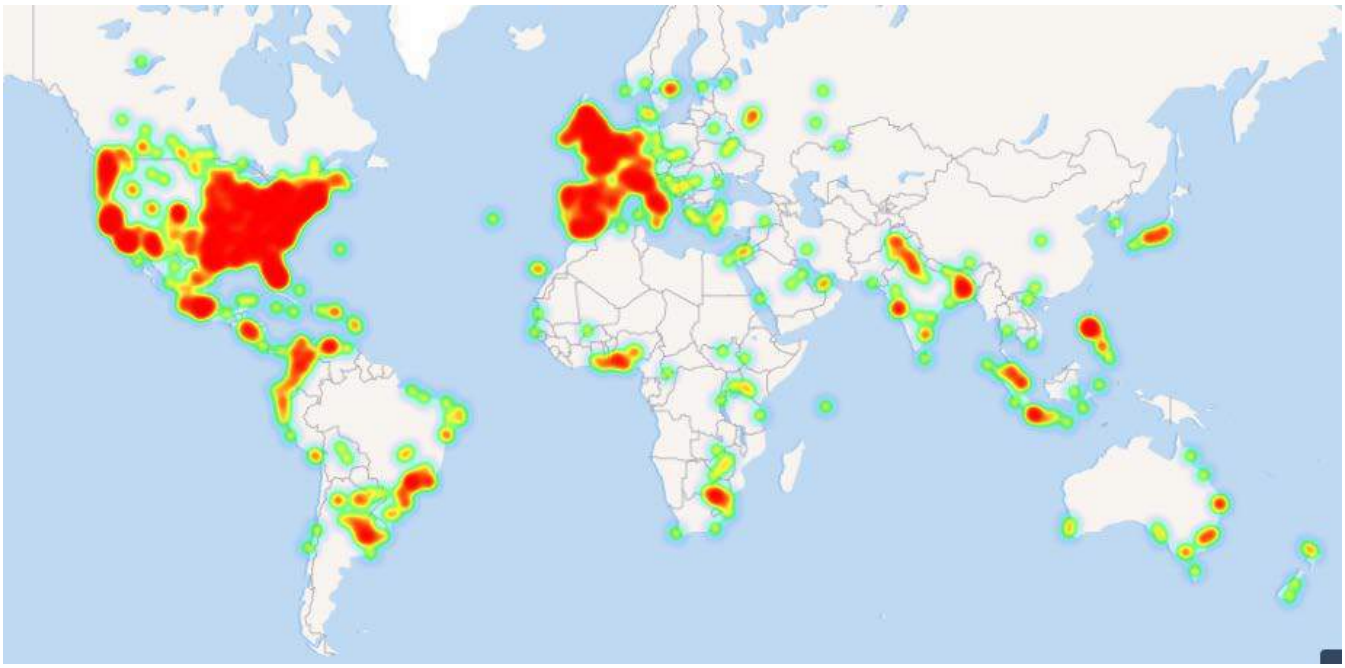


Figure 4: Mapa de calor de tweets que representa la monitorización de 5 semanas.

Para tener una visión clara de la difusión de los partidos en Twitter, creamos una búsqueda formada por las mayores ligas deportivas a nivel mundial y terminología relacionada con la difusión de contenidos. Como hemos dicho anteriormente, este análisis cubre un periodo de cinco semanas; del 1 de noviembre al 10 de diciembre del 2018.

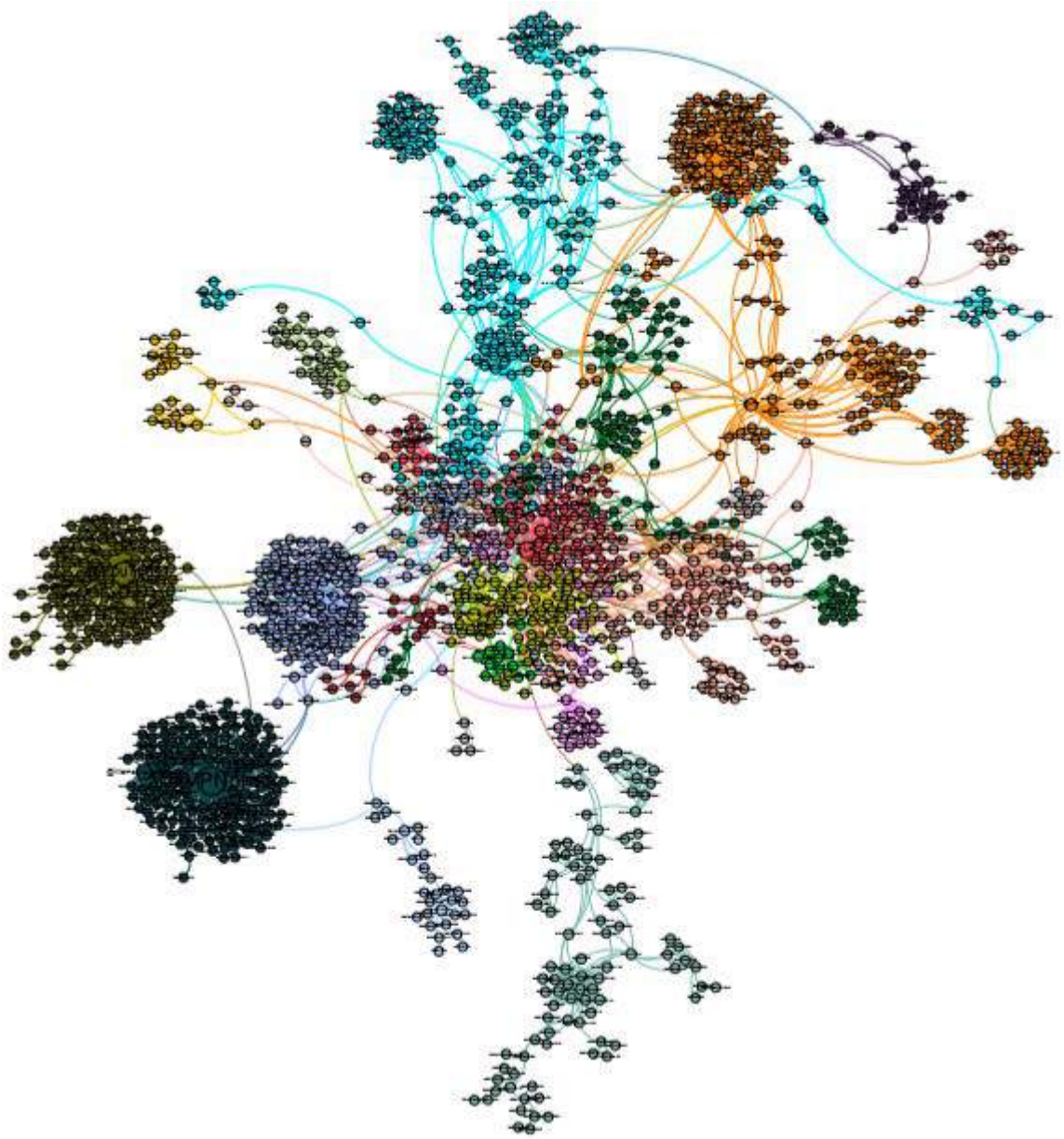
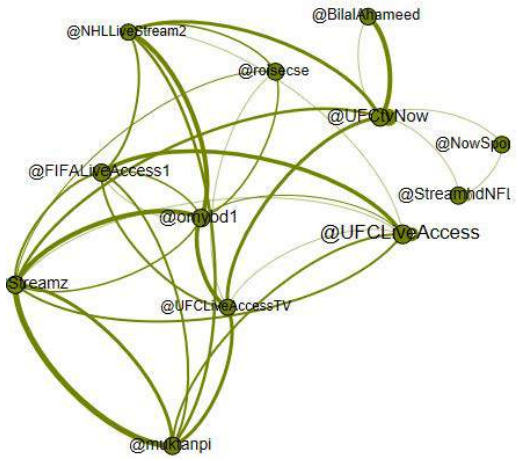
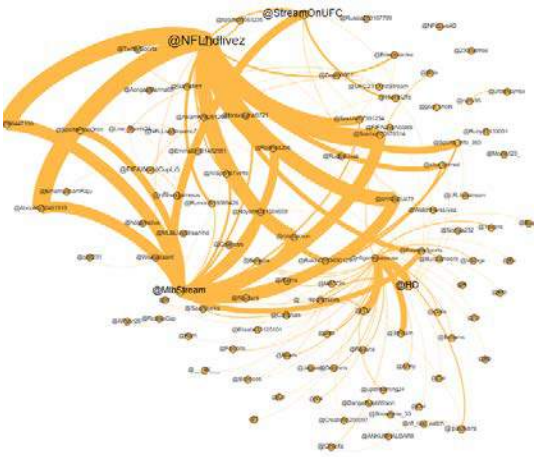


Figura 5: Conversación de Twitter acerca de retransmisiones de varios deportes

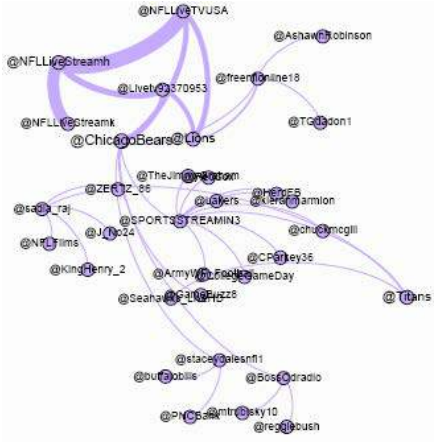
En esta conversación, hemos identificado 5 botnets de difusión de contenidos:



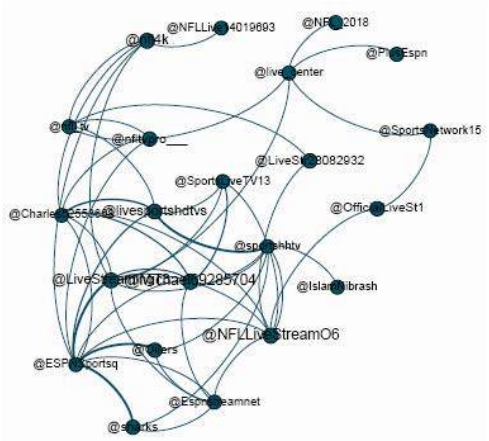
Botnet 1: Esta botnet cubre UFC, hockey y béisbol. La botnet estaba formada por 12 perfiles y todos ellos siguen activos.



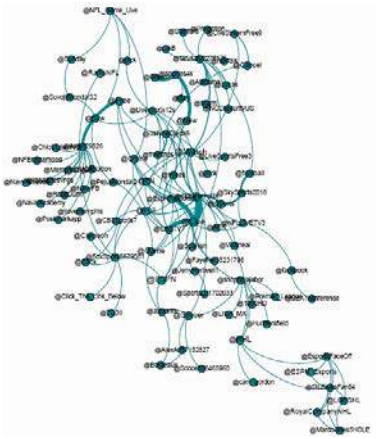
Botnet 2: Esta botnet cubre principalmente las ligas europeas. De 96 perfiles iniciales, 4 han sido borrados/suspendidos.



Botnet 3: Esta botnet cubre el streaming de la NFL y la AFL. De los 22 perfiles iniciales, 21 siguen activos.



Botnet 4: Esta botnet cubre el boxeo, el streaming NFL y MLB. Estaba formado por 46 perfiles y 45 siguen activos.



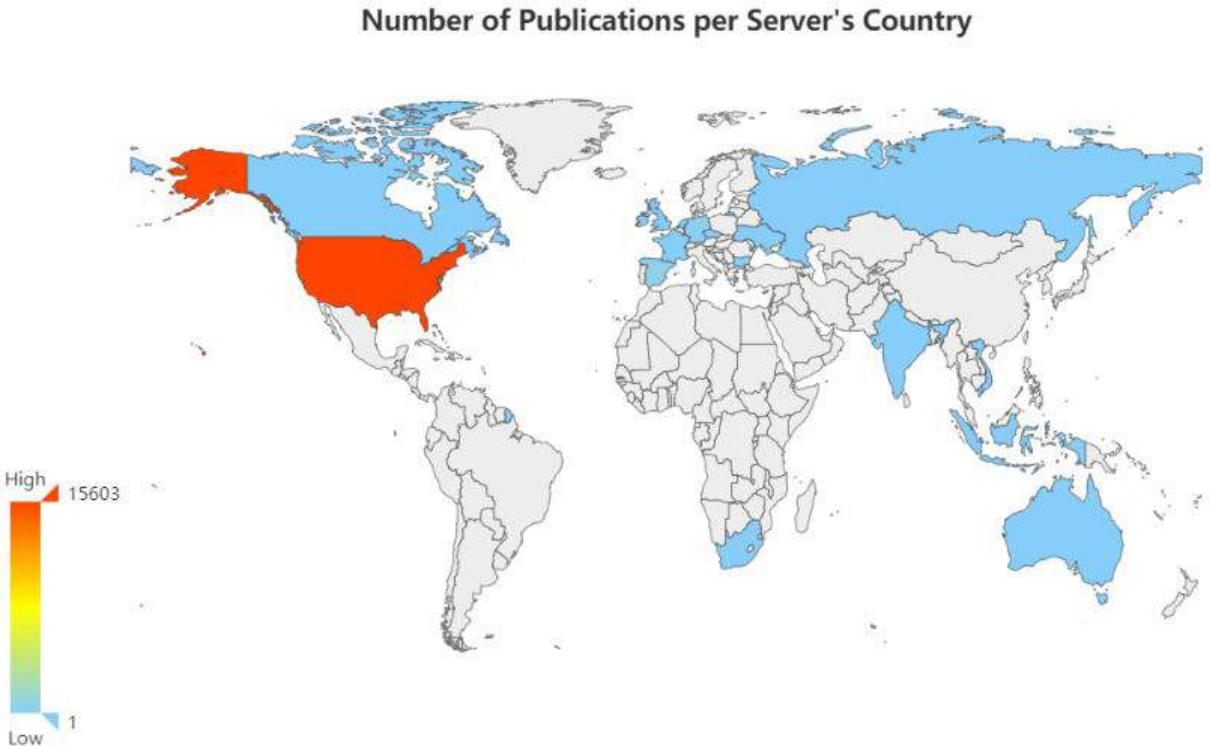
Botnet 5: Esta botnet cubre el fútbol americano y las ligas europeas. Estaba formado por 187 perfiles y 183 siguen activos.

Figura 6: Botnets de Twitter

Al comparar el perfil del Mundial y el análisis reciente, podemos ver que **25 perfiles de bot** coinciden y han estado activos y compartiendo contenido de streaming desde junio de 2018. Específicamente, la botnet número 2 del último análisis tiene la mayor parte de la botnet número 4 de la Copa Mundial de la FIFA (doble tamaño).

Además del análisis de los botnets de la conversación, hemos analizado las direcciones IP de los sitios web de streaming distribuidos en los tweets.

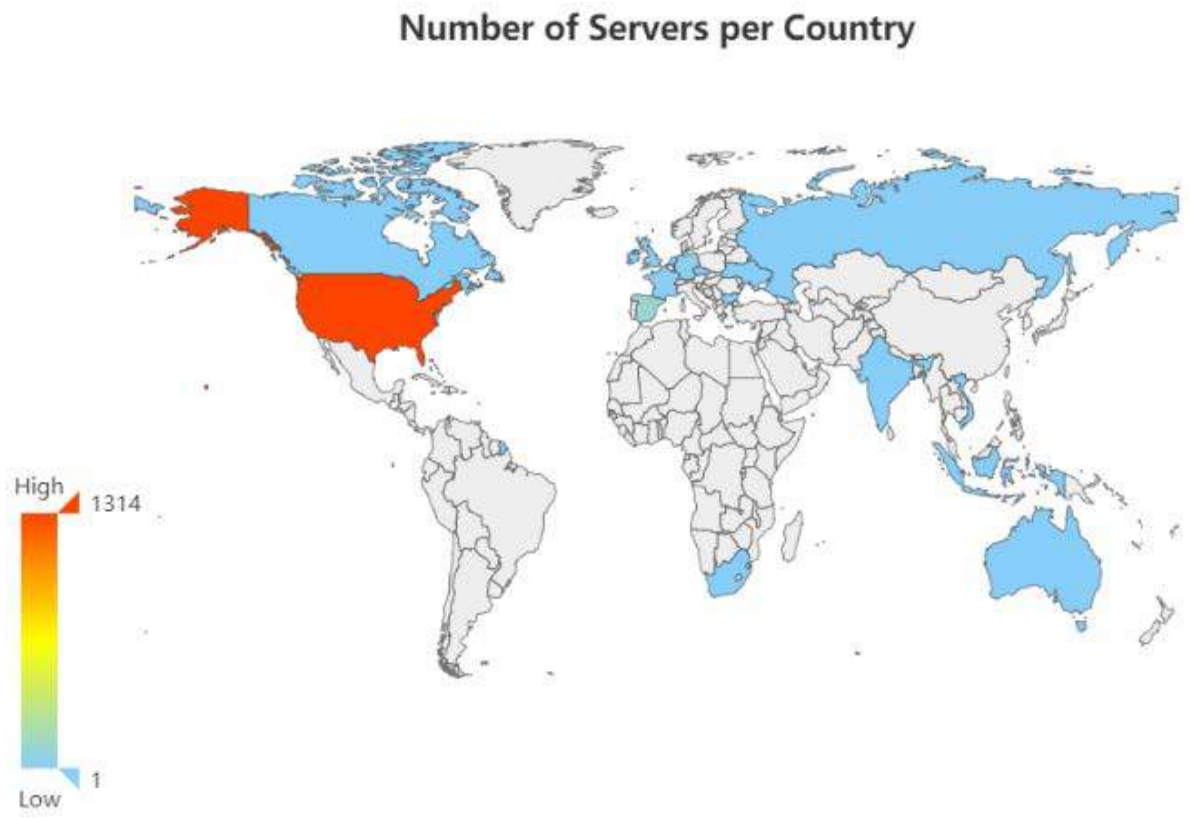
En primer lugar, hemos analizado el número de publicaciones (enlaces) por país del servidor.



United States:	15603	**United Kingdom:**	76	**Ukraine:**	39	**Canada & Ireland:**	4
Spain:	525	**South Africa:**	63	**Russia:**	15	**Vietnam:**	3
Germany:	359	**France:**	57	**Indonesia:**	7	**Australia:**	2
Seychelles:	80	**Netherlands:**	40	**Singapore:**	5	**Bulgaria & Czech Rep**	1

Figura 7: Cifras de publicaciones por servidor en cada país.

Hemos identificado también el número de servidores por país:



United States:	1314	**France:**	18	**Indonesia & ZA & Singapore & Canada:**	3
Spain:	112	**Ukraine:**	12	**Seychelles & India & Australia:**	2
Germany:	40	**Netherlands:**	11	**Bulgaria & Czech Rep & Vietnam:**	1
United Kingdom:	34	**Russia & Ireland:**	4		

Figura 8: Número de servidores por país

Cuando comparamos los últimos dos gráficos, podemos observar 2 servidores ubicados en Seychelles que emiten ilegalmente 80 enlaces diferentes como también en los Países Bajos, cada servidor emite un promedio de 4 enlaces de contenido ilegal.

5.1. Ejemplos de Tweets

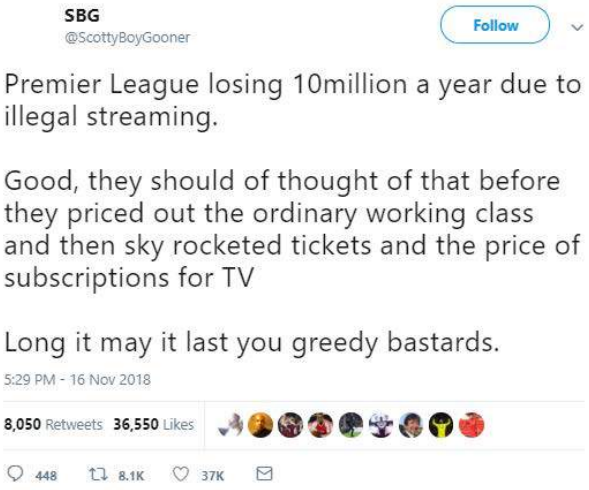


Figura 9: Tweet de un usuario normal quejándose de los elevados precios de las retransmisiones legales.

Figura 10: Tweet con un enlace a una retransmisión ilegal de la Copa Libertadores

Figura 11: Tweet promoviendo retransmisiones ilegales de la NFL

Figura 12: Tweet promocionando diversos servicios ilegales de retransmisión de eventos deportivos

6. Conclusiones

- Con Aldara hemos sido capaces de identificar botnets en Twitter basados en las formas de los grafos y gracias a sus algoritmos.

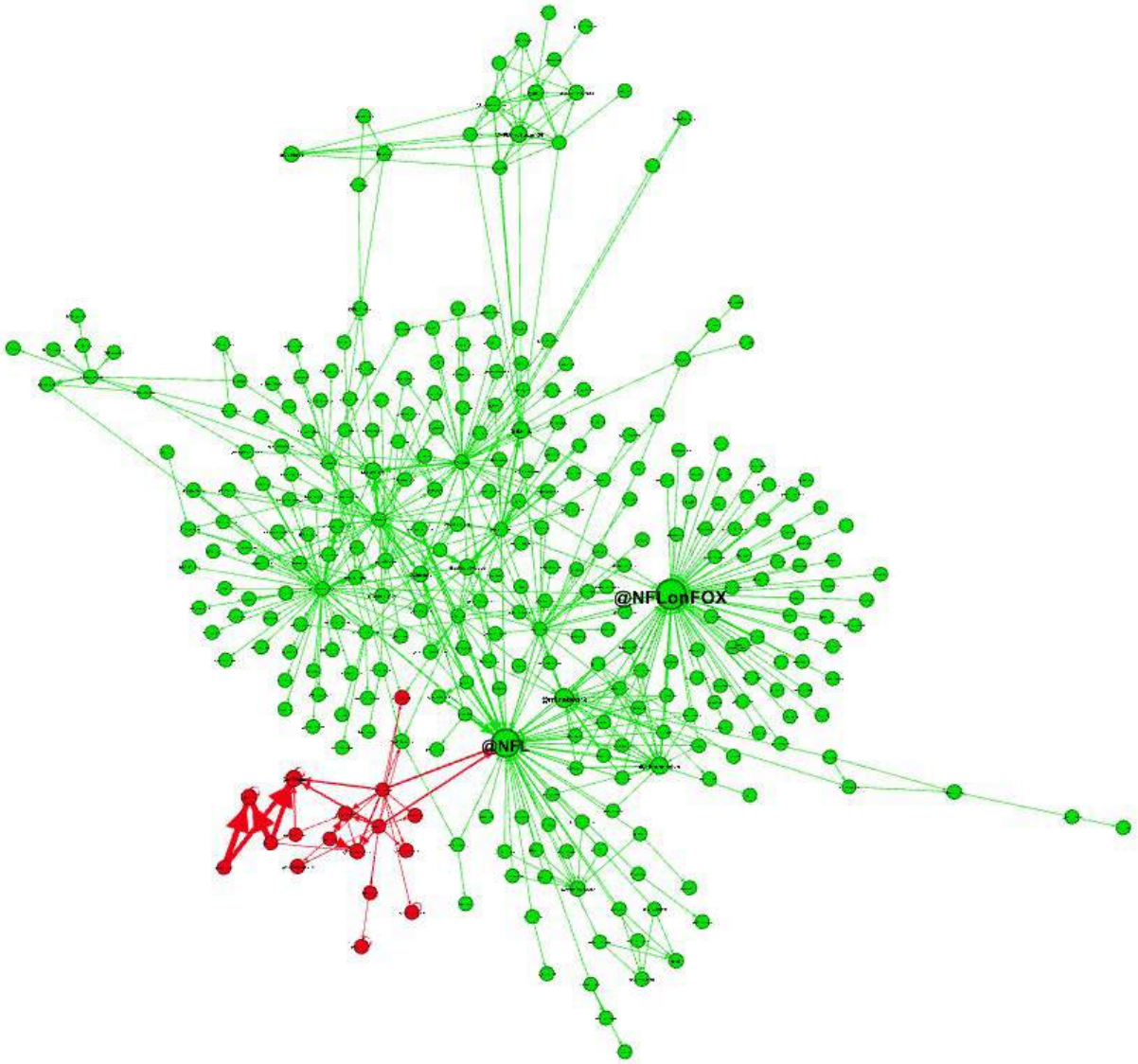


Figura 13: Grafo de Twitter (El color rojo representa una botnet)

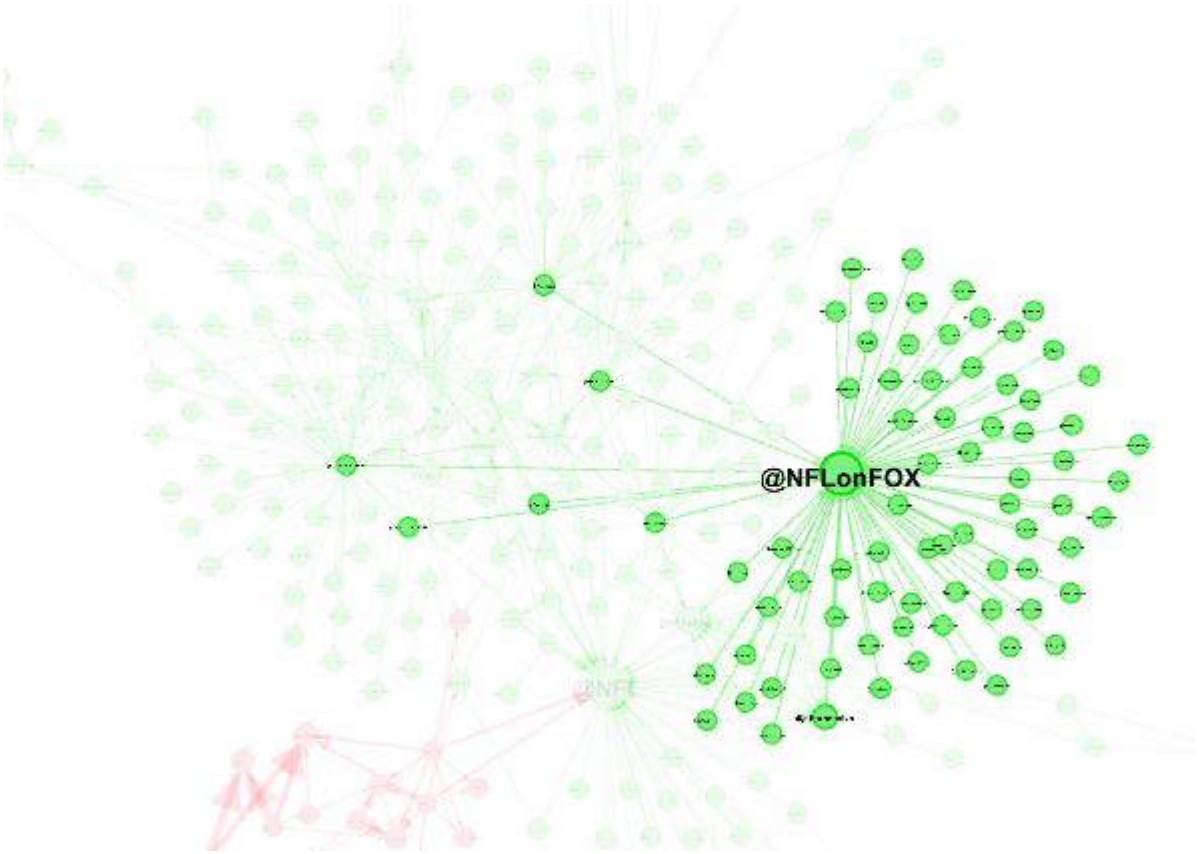


Figura 14: Comportamiento habitual de una retransmisión legal (comportamiento unidireccional)

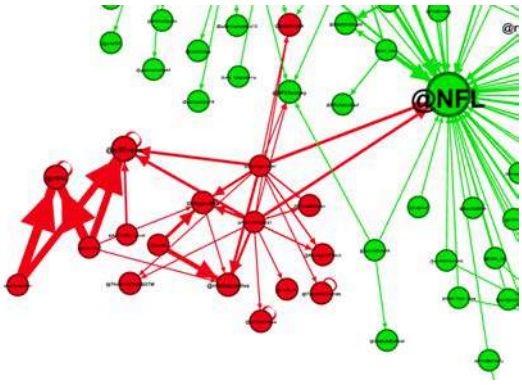


Figure 15: Botnet de Twitter (caótica y multidireccional)

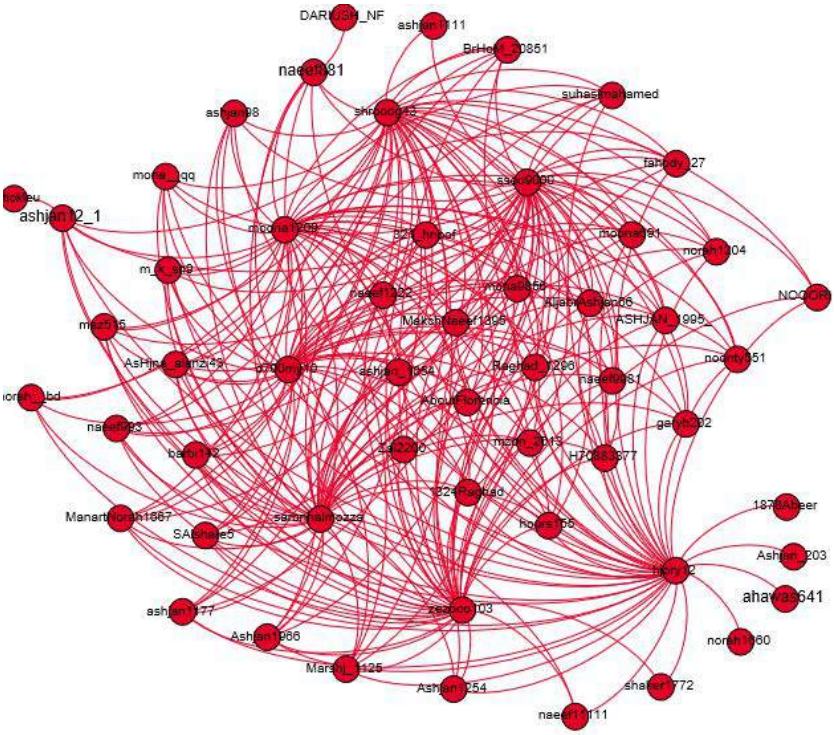


Figura 16: Otra imagen que representa la forma típica de una botnet

- Las botnets de Twitter **no suelen** centrarse en un deporte en particular, sino que consideran que se puede promover la difusión ilegal de cualquier acontecimiento relevante.

- El tamaño de las botnets varía; la botnet más grande estaba compuesta por 183 perfiles y la más pequeña por 12 perfiles.

- Durante las **5 semanas de seguimiento**, el **porcentaje medio** de tweets relacionados con la difusión ilegal por deporte es:

  Fútbol americano: **0,53%** (45.756 tweets)
  Rugby: **0,15%** (1.200 tweets)
  Fútbol: **0,14%** (53.304 tweets)
  Baloncesto: **0,07%** (9.132 tweets)
  Béisbol: **0,06%** (2.381 tweets)
  Cricket: **0,03%** (333 tweets)

- Los tres países que más contenido ilegal difunden son Estados Unidos, España y Alemania.

- Como era de esperar, los tweets con enlaces a webs de streaming ilegales de futbol son más comunes que los de demás deportes.

Figura 17: Tweets con enlaces incrustados están relacionados más frecuentemente con el fútbol que con el resto de los deportes.

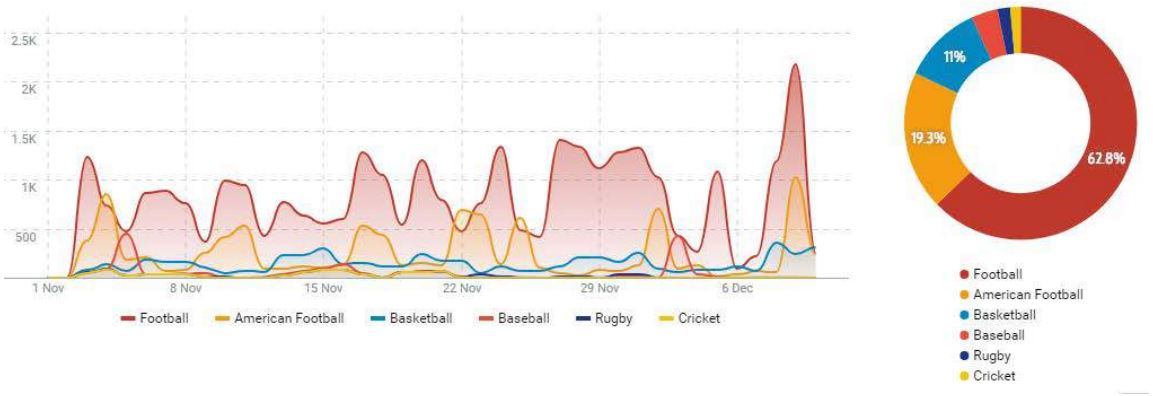


Figura 17: Tweets con enlaces incrustados están relacionados más frecuentemente con el fútbol que con el resto de los deportes.

7. Consejos

- Para evitar este tipo de difusión ilegal, la TSA (Telco Security Alliance) dispone de diferentes métodos para luchar contra este delito cibernético en particular que incluye desde procedimientos específicos con los principales ISPs del mundo para realizar las tomas necesarias hasta la inversión en start-ups como Smart Protection (http://smartprotection.com/) que trabaja para proteger la propiedad intelectual y el uso indebido de sus contenidos digitales.

- También hemos utilizado los algoritmos de Aldara en crisis de reputación y nos ha ayudado a eliminar el "ruido" artificial (botnets o cuentas automáticas). Este tipo de **limpieza** conduce a un análisis de fondo de la conversación e **identifica el alcance real de una crisis**.

8. Glosario

- **Atacante**: actor cuya actividad incluye ciberataques contra los activos de una empresa o gobierno.
- **Behavioral Flamingo Score (BFS)**: Métrica desarrollada por ElevenPaths para medir la influencia de cualquier perfil en una red social. Se basa en la forma en que otros perfiles interactúan con el perfil evaluado.
- **Emisor**: actor cuya actividad se centra principalmente en la difusión de mensajes en lugar de realizar cualquier tipo de ataque.
- **Conversación**: grupo de tweets asociados al mismo tema.
- **Gráfico de conversación**: representación gráfica de una conversación (ver Conversación).
- **Influencer**: Individuo que tiene el poder de afectar a las decisiones de otros debido a su autoridad, conocimiento, posición o relación (real o percibida).
- **Perfil**: concepto asociado a un usuario de una red social.
- **Gráficos de Usuarios**: es la representación gráfica de las relaciones sociales (ver Relación Social) a partir de uno o más perfiles y dando 2 o más pasos. Es decir, desde el usuario A, 1 paso devolvería cada relación de ordenación desde y hacia el perfil B. Un segundo paso devolvería cada relación de ordenación desde y hacia cada perfil obtenido en el paso 1 y así sucesivamente.

Acerca de la Telco Security Alliance

La alianza, compuesta por Telefónica, Etisalat, Softbank y Singtel, es uno de los mayores proveedores de seguridad cibernética del mundo, con más de 1.200 millones de clientes en más de 60 países de Asia Pacífico, Europa, Oriente Medio y América. A través de sus recursos y capacidades combinadas, el grupo puede proteger a las empresas contra los crecientes riesgos de ciberseguridad a medida que el entorno de seguridad de la información se vuelve cada vez más complejo.

A través de la alianza, los miembros pueden lograr sinergias operativas y economías de escala que, con el tiempo, ayudarán a reducir los costos para sus clientes. Los miembros del grupo operan 22 Centros de Operaciones de Seguridad (SOCs) de clase mundial y emplean a más de 6.000 expertos en seguridad cibernética. Para ampliar su presencia global, la alianza está abierta a la incorporación de nuevos miembros con el tiempo.

Bajo el acuerdo, el grupo compartirá la inteligencia de la red sobre las amenazas cibernéticas y aprovechará su alcance global conjunto, sus activos y sus capacidades de seguridad cibernética para servir a los clientes de todo el mundo. Aprovechando la huella geográfica y la experiencia de cada miembro, la alianza es capaz de apoyar a los clientes de los demás en cualquier lugar y en cualquier momento, permitiéndoles responder rápidamente a cualquier amenaza de seguridad cibernética.

Para mejorar su cartera de seguridad cibernética, los miembros también estudiarán la posibilidad de desarrollar nuevas tecnologías, como el análisis predictivo mediante el aprendizaje automático y la seguridad cibernética avanzada para la Internet de los objetos. La alianza también considerará el desarrollo de una hoja de ruta conjunta para la evolución de sus carteras de seguridad y explorará inversiones conjuntas en productos y servicios de seguridad, SOCs, plataformas, start-ups e I+D.