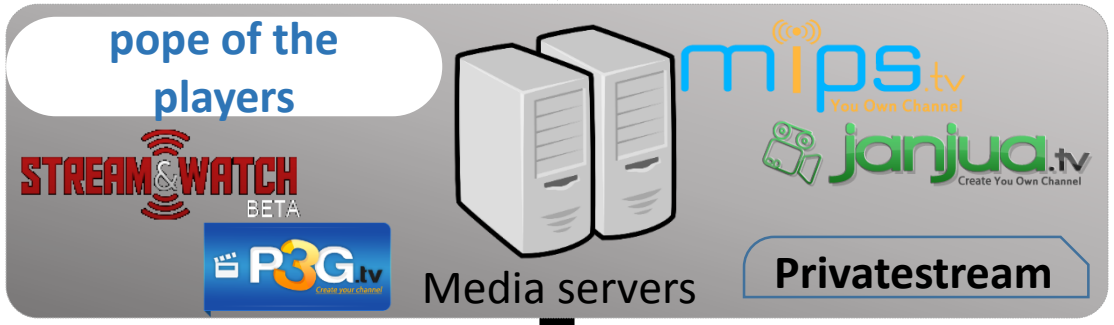
It’s Free for a Reason: Exploring the Ecosystem of Free Live Streaming Services

M. Zubair Rafique, Tom Van Goethem, Wouter Joosen,
Christophe Huygens, and Nick Nikiforakis
iMinds-DistriNet, KU Leuven
Stony Brook University

Media stream



Your channel has been successfully created. Use the details below to broadcast:

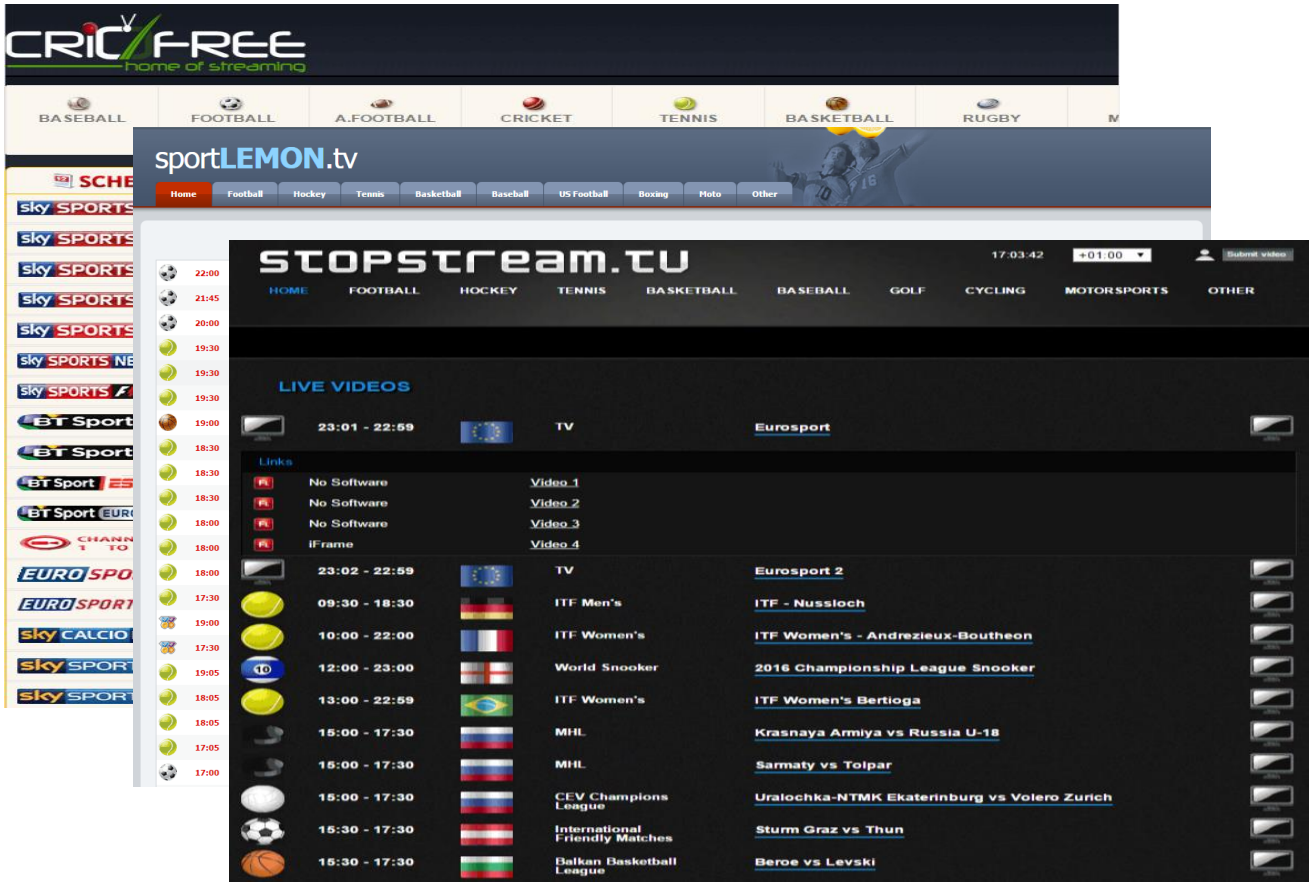
P3G.tv

Download	Download Flash Media Live Encoder 3.2
FMS URL	rtmp://p3gpublish.com/live
Stream Name	flis_illegal?key=dc8e8e6c&id=12174
Start	Click **Start**
Channel page:	http://www.p3g.tv/flis_illegal
Channel stats:	http://www.p3g.tv/dc8e8e6c

Embed Code:

```
<script type='text/javascript'> width=500, height=400, channel='flis_illegal',
```

In case of any issue, please contact our live support
Skype: p3g.tv
email: p3gcontact@gmail.com



Rojadirecta

Rojadirecta.me has received an estimated 5,836,000 visits over the last 30 days.

http://www.trafficestimate.com/rojadirecta.me

Global Rank

2,497 ▼ 862

Rank in Mexico

247

Threat to Industry

Premier League wins piracy block of First Row Sports

By Dave Lee
Technology reporter, BBC News

17 July 2013 | Technology

The Premier League has won a court order forcing UK internet service providers to block a popular football streaming website.

The site will be blocked in time for the next Premier League season

FirstRow1.eu, operated from Sweden, links to various video streams showing football from around the world - a breach of copyright, the High Court ruled.

It will be blocked ahead of the new season, which begins next month.

It is the first time a sport-related website has been blocked in the UK.

It follows a raft of site blocks put in place by the music industry, which is increasingly using ISP-level filtering to cut off access to popular sites offering free downloads illegally.

However, this case marks the first time a site simply facilitating access to streaming sites - rather than hosting streams themselves - has been blocked.

'£10m a year'

"It is absolutely imperative that content industries are afforded protection under the law if they are to continue investing in the sort of quality talent and facilities that have made them successful and of interest in the first place," a spokesman for the Premier League said.

Technology NEWS › TECHNOLOGY

May 24, 2015

Web pirates are stealing from sports broadcasters

First music, then movies. Now it's the sports industry that's about to get disrupted by the Web.

By Aaron Elstein

Web pirates are playing offense against the $60 billion U.S. sports industry.

This Week in Crain's New York: May 25, 2015

Listen to the Podcast or

If you've followed the Rangers' quest for the Stanley Cup, then you've had a few options if you've wanted to watch.

You could buy a ticket, though the cheapest seats for playoff

GET CRAIN'S DIGITAL NY

Sign up for our FREE w email newsletter. New growing tech sector, w and executive moves.

Enter your email add

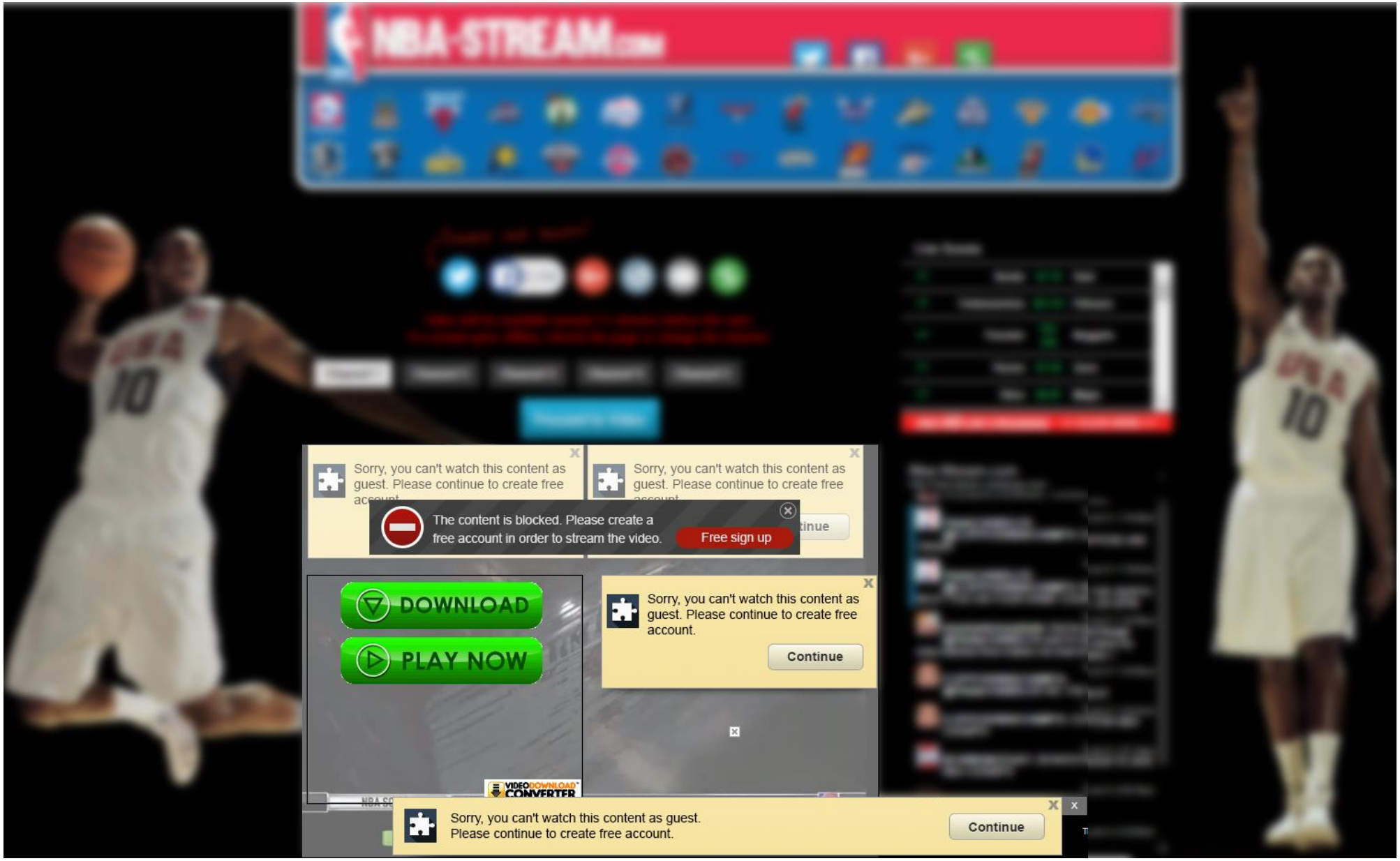
CRAIN'S AUTHORS

Aaron E

@InTh

LATEST | MOST POPUL

Threat to User Security



Exploring the FLIS Ecosystem

- **Goal: Highlight the negative effect of Free Live Streaming (FLIS) on users and map the ecosystem of FLIS services**

- Our approach:
  - Analyze sports-specific, web-based FLIS services
  - Develop an infrastructure to gather FLIS domains
  - Inspect network traffic to identify parties providing media-servers
  - Examine deceptive advertisement practices

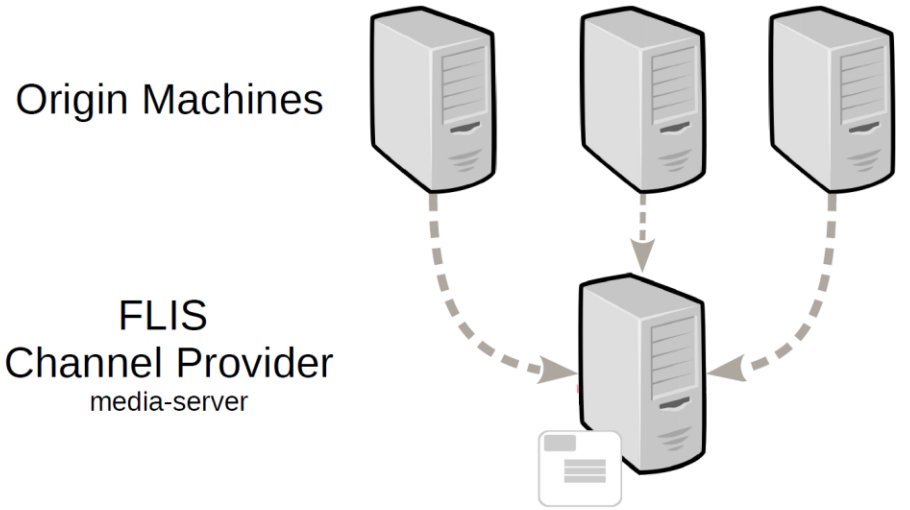
- Insights into the FLIS ecosystem:
  - Automatic identification of FLIS parties
  - Possible copyright and trademark infringements
  - Threat to user security

Outline

- Background on FLIS ecosystem
- Data gathering and identification
- Several aspects and practices of FLIS services
  - Hosting preferences of FLIS parties
  - Possible copyright and trademark infringements
  - Substandard, deceptive, and unavoidable advertisement
  - Exposing users to malware websites
  - Additional malicious activities (link hijacking, malware distribution)

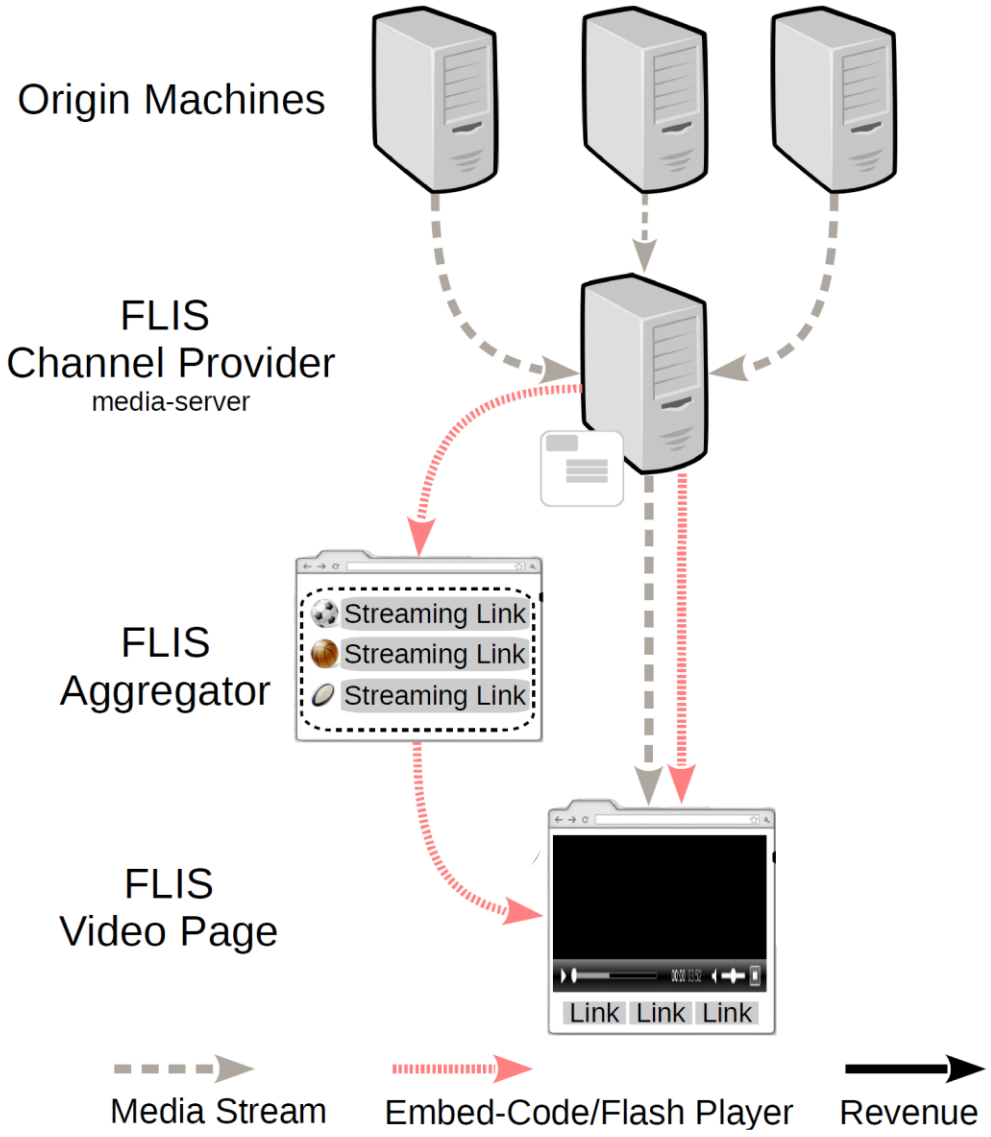
FLIS Ecosystem

- Channel providers
  - Provide media servers for free anonymous broadcasts of live streams
  - Maintain websites to facilitate the process
  - Provide stream-embedding code
- Aggregators
  - Catalog stream-embedding codes
  - Index various FLIS links
- Advertisers and ad networks
  - Provide ad scripts
  - Fetch and display ads from different advertisers
  - Pay channel providers and aggregators



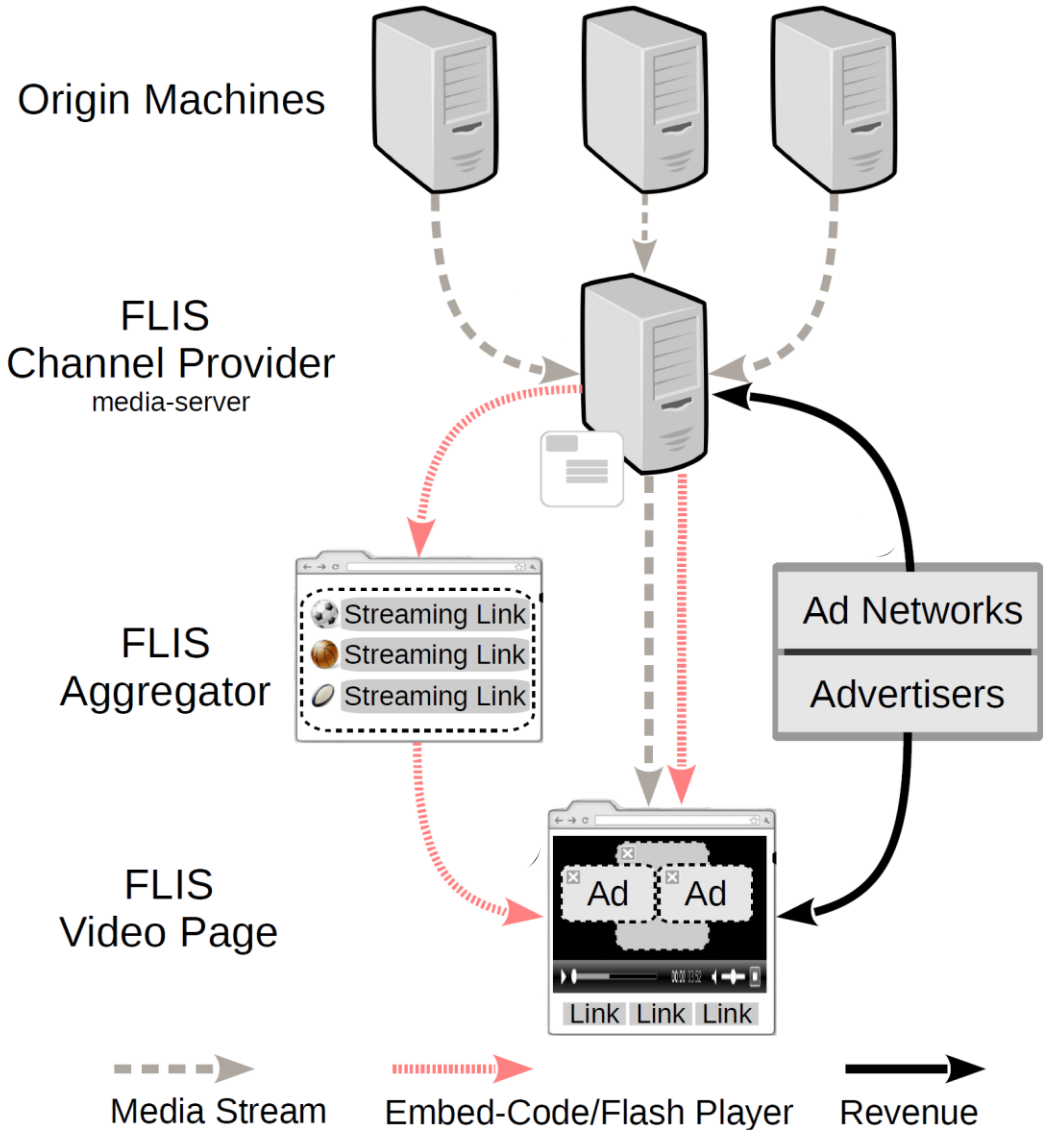
FLIS Ecosystem

- Channel providers
  - Provide media servers for free anonymous broadcasts of live streams
  - Maintain websites to facilitate the process
  - Provide stream-embedding code
- Aggregators
  - Catalog stream-embedding codes
  - Index various FLIS links
- Advertisers and ad networks
  - Provide ad scripts
  - Fetch and display ads from different advertisers
  - Pay channel providers and aggregators



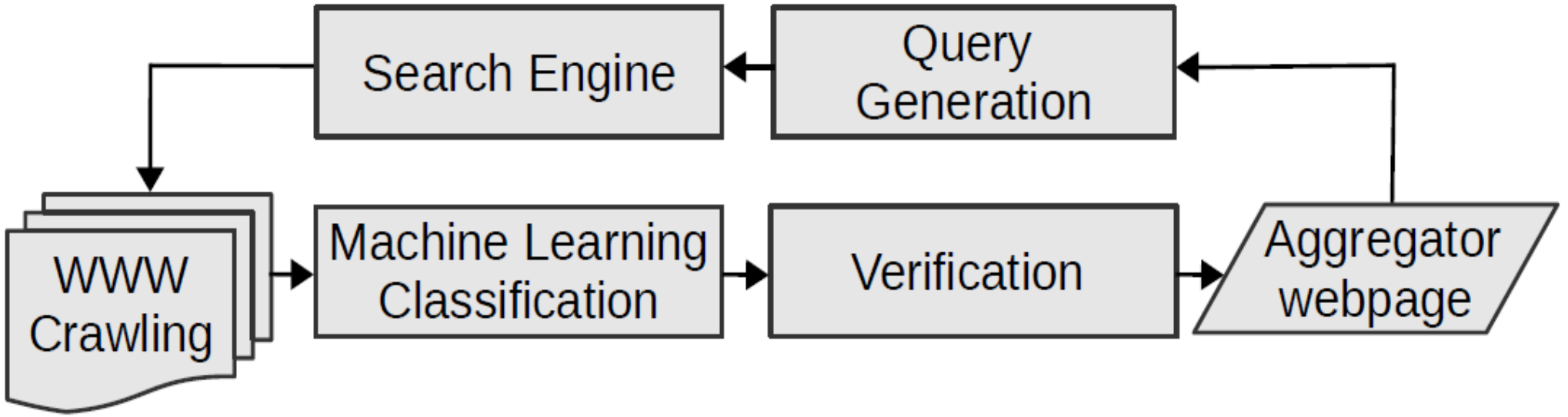
FLIS Ecosystem

- Channel providers
  - Provide media servers for free anonymous broadcasts of live streams
  - Maintain websites to facilitate the process
  - Provide stream-embedding code
- Aggregators
  - Catalog stream-embedding codes
  - Index various FLIS links
- Advertisers and ad networks
  - Provide ad scripts
  - Fetch and display ads from different advertisers
  - Pay channel providers and aggregators



Data Gathering and Identification

Collecting Aggregator Domains



Seeds: 500 aggregator domains

SE URLs: 513,324

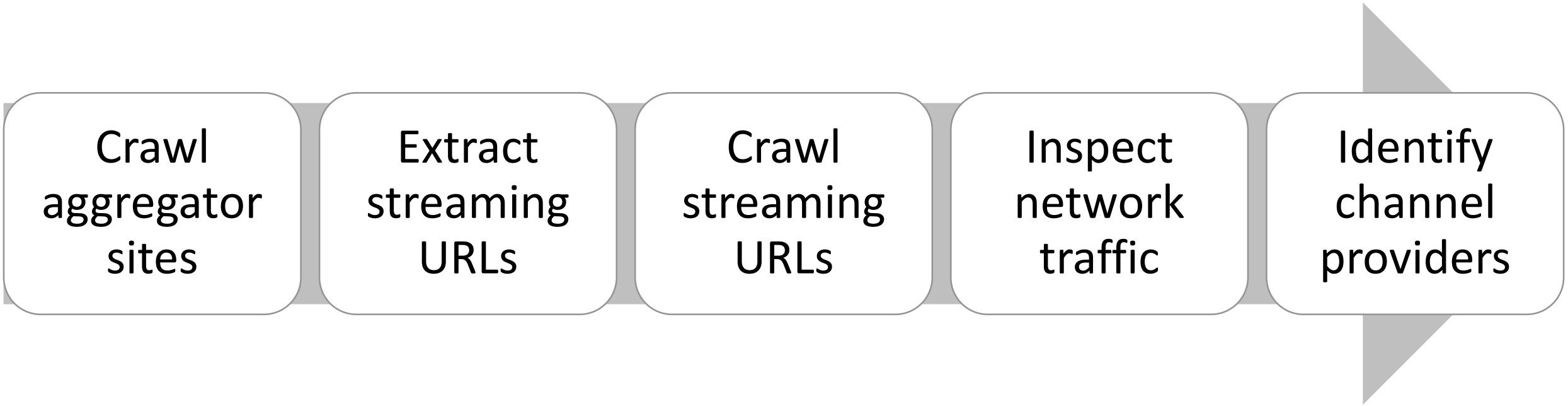
URLs classified: 23,549

Verified: 5,685 aggregator domains

All your iframes point to us
N. Provos, M. Panayiotis, M. A. Rajab, F. Monrose. Usenix Security 2008.

EvilSeed: A guided approach to finding malicious web pages
L. Invernizzi, P. Milani, S. Benvenuti, C. Kruegel, M. Cova, G. Vigna. Oakland 2013.

Identification of Channel Providers



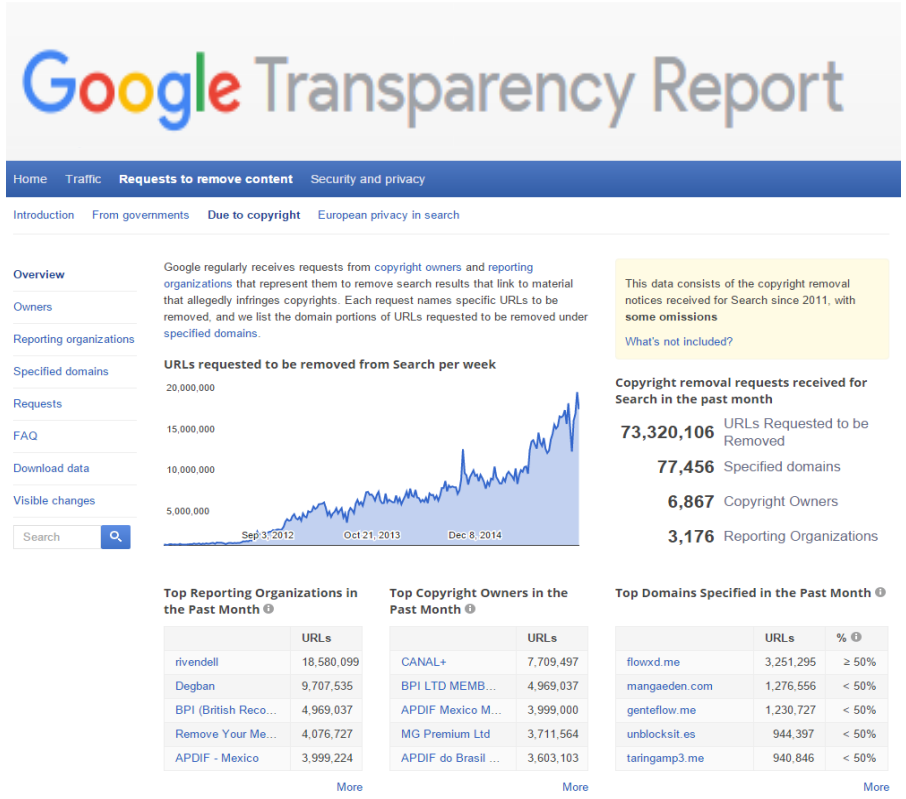
Inspected domains: 1,000 aggregator domains
Inspected traffic: 1 TB
Streams found: 52,469
Channel providers: 309

Top Hosting Companies' Infrastructure Employed by the Channel Providers

Hosting Company	Hosting Country	# Channel providers	% Streams
privatelayer.com	Switzerland	14	11.7%
koddos.com	Belize	11	24.2%
ecatel.net	Netherlands	10	12.7%
ovh.ca	Canada	10	1.2%
Portlane.com	Sweden	7	10.5%

Possible Copyright and Trademark Infringements

Possible Copyright Infringements



- 30.0% (1,706/5,685) of aggregator domains have been reported at least once by copyright owners.
- 64.4% (199/309) of channel providers have been reported at least once by copyright owners.

Possible Trademark Infringements

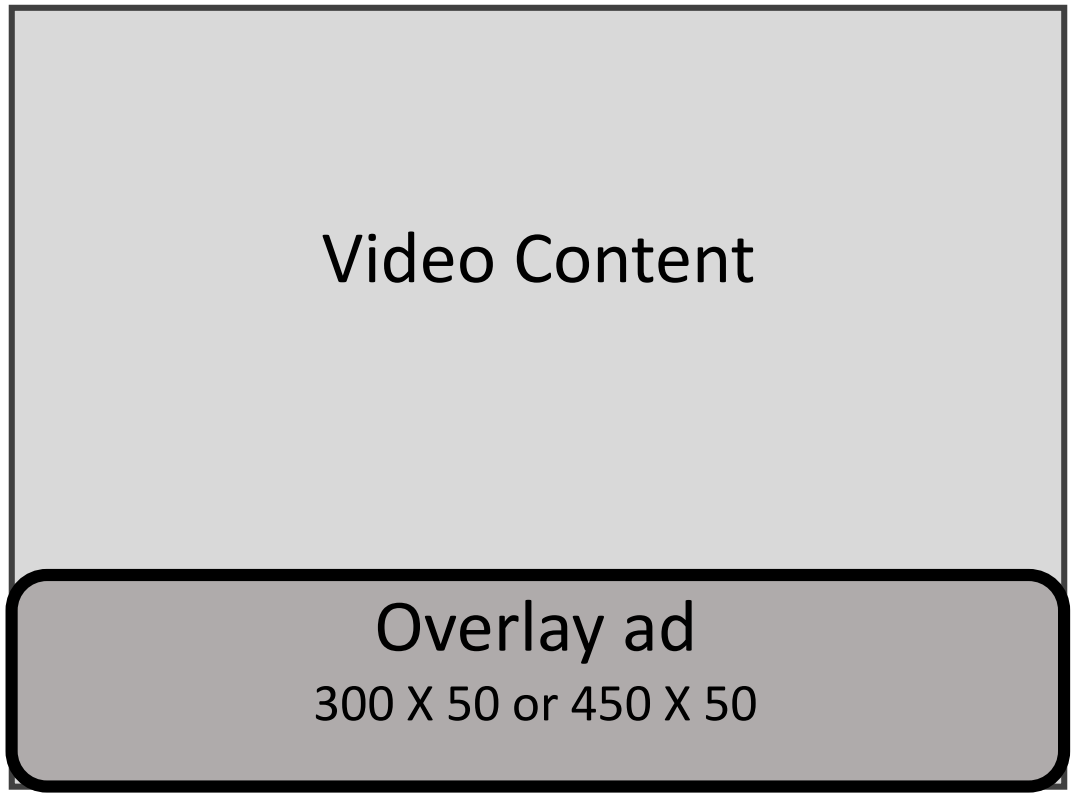
- 7.72% (439/5,685) of aggregator domains use trademarks of well known sports TV channels, leagues, and organizations in their domain names. (e.g., skysportslive.tv, skyembed.com).

- 4.9% (282/5,685) of aggregator domains utilize the trademark logos of popular sports TV channels.

Substandard, Deceptive, and Unavoidable Advertisement

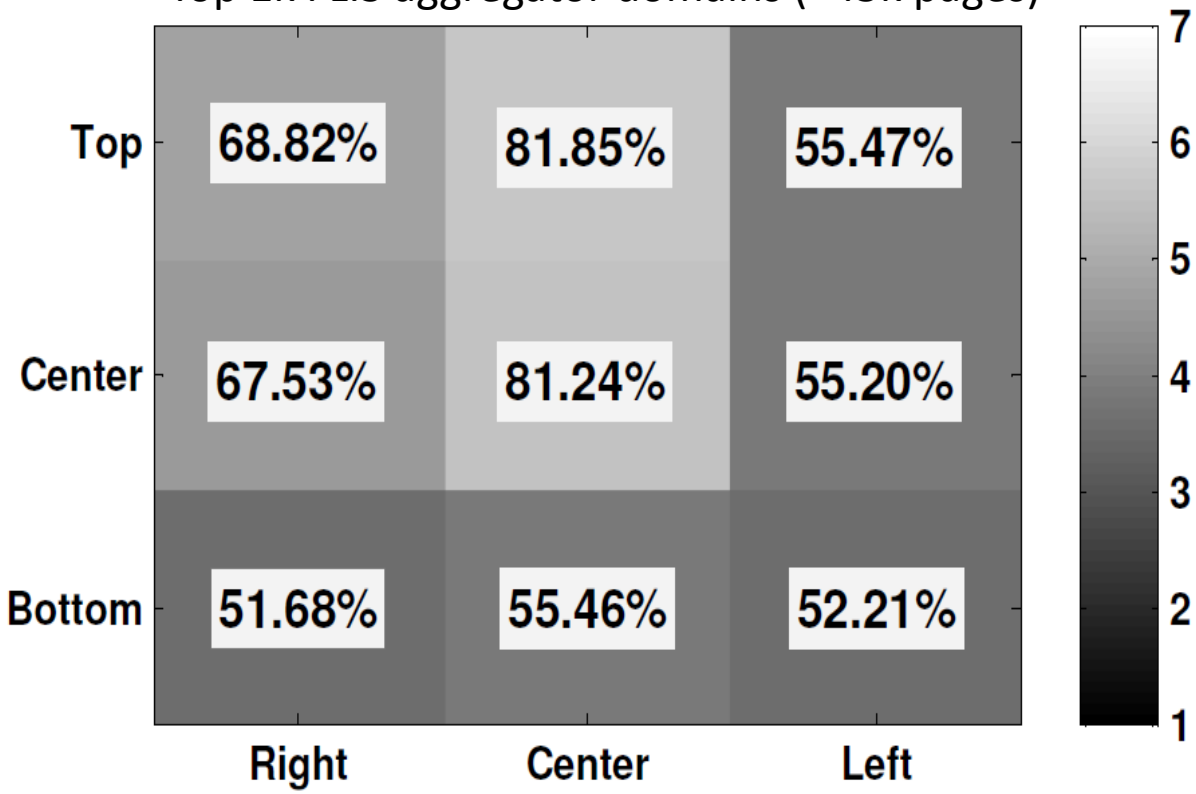
Substandard

IAB Standard



"The overlay ad should not be more than 1/5 of the height of the player."

Top 1k FLIS aggregator domains (~45k pages)



93% of the video players were stuffed with overlays, hiding more than 80% area of the player.

Digital video in-stream ad format guidelines and best practices. 2008
http://www.iab.net/media/file/IAB-Video-Ad-Format-Standards.pdf

Deceptive

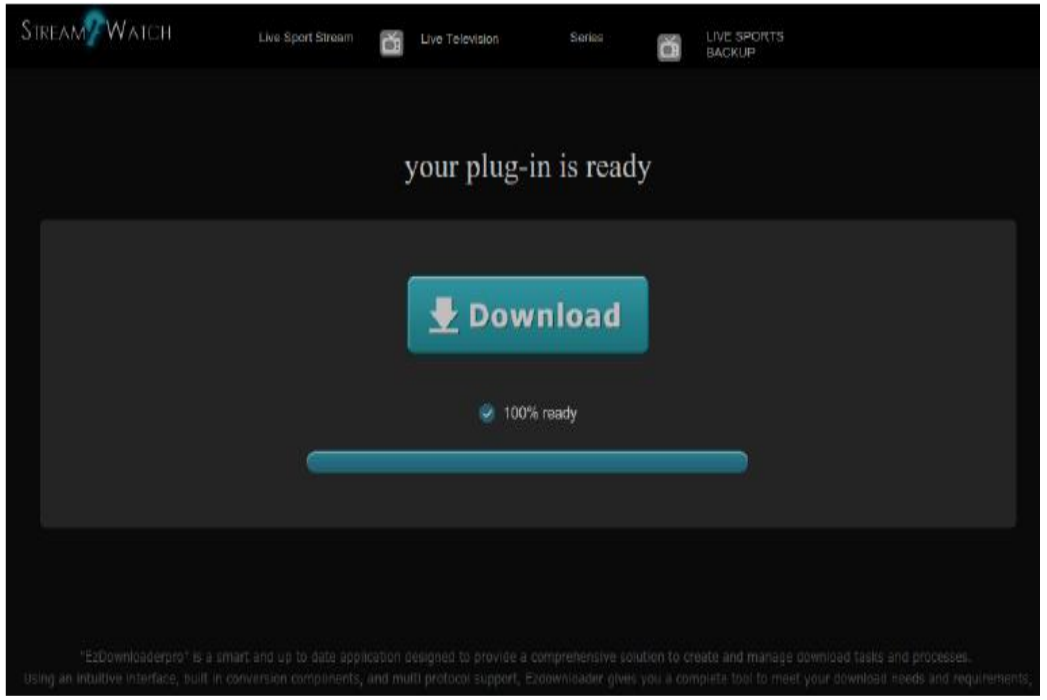

An additional plugin is required to display the video in this page
Install plugin
X
NEXT LINK
Download
Play now
Watch in
System Update
Flash Player is outdated
To improve streaming quality please update to latest version of flash player.
Current version: 12.0.0.77
Latest Version: 12.0.0.78
Update
Details...
SKIP >>>
00:00
00:00

Unavoidable

- Out of the top 1K investigated aggregator domains, 16.3% (163/1,000) employed scripts that attempt to detect and defeat the ad-blockers.
  - antiblock.org
  - advertisement.js

Exposing Users to Malware Websites

Automated Interaction with Overlay ads



- Crawled FLIS video pages
  - automatically identify and click overlay ads
  - log network traffic
  - capture screenshots of ad pages
- Collected screenshots of 30,354 ad pages (top 1,000 aggregator domains), cluster the screenshots, and manually labeled each cluster.
- 50% of the time, a click on an overlay ad leads to a malware-hosting webpage (offers malware binary or malicious browser extension).

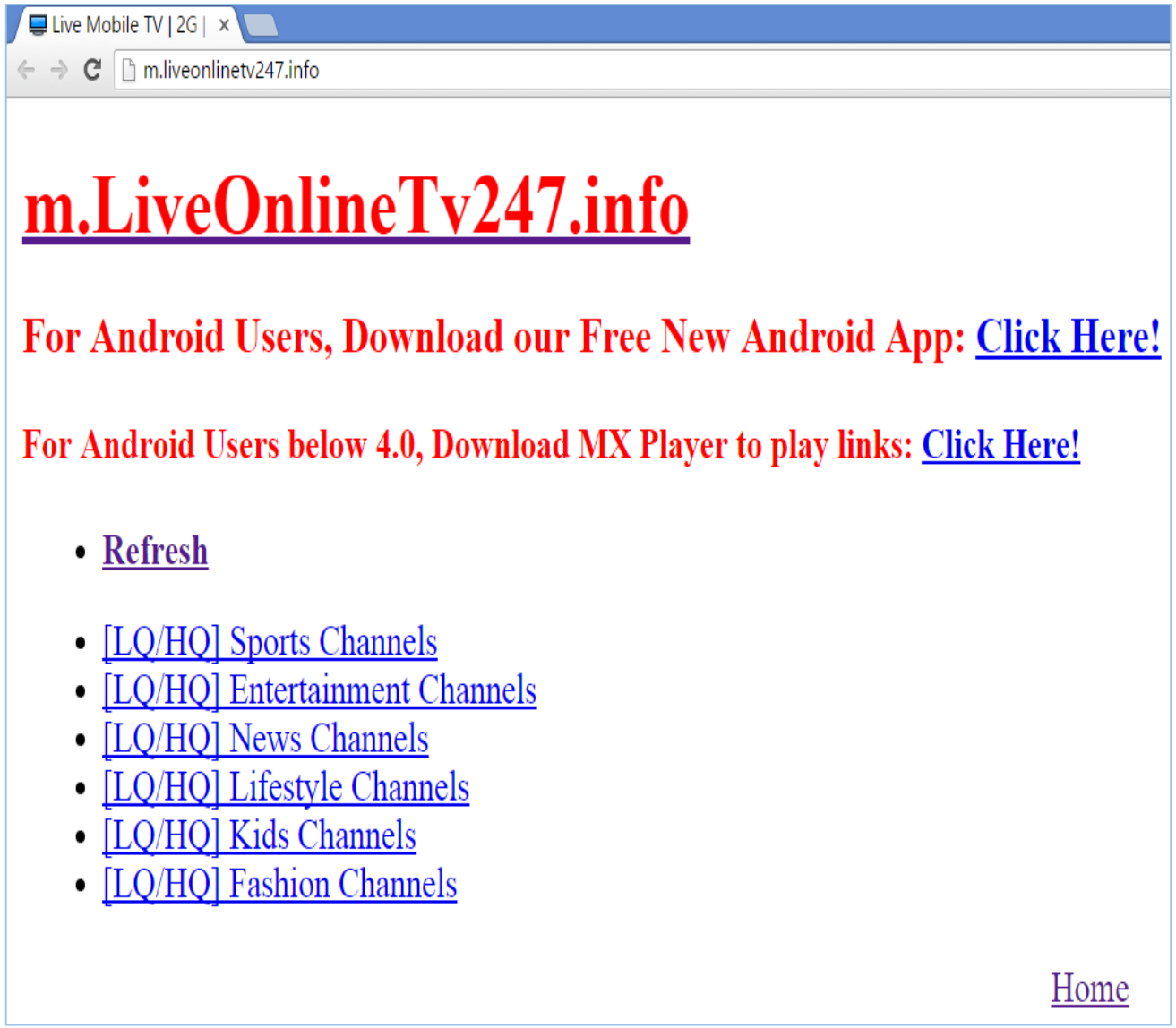
Malware Distributors

	Top Advertisers
1.	3c41ddc0.se
2.	s.ad[0-9]{3}m.com
3.	creative.ad[0-9]{3}m.com
4.	ad.directrev.com
5	vipcpms.com

- 12,683 malware payloads, 1,353 distinct binaries.
- 11 malicious Chrome extensions from the ad websites opened after clicking on the overlay ads.

Additional Malicious Activities

Immediate Distributor of Malware



virustotal

SHA256: f3d1d26781dd559198f6ddc3d9c95ac0e7ed93e5a75bebcd3ab8161d4b5e9bf6

File name: LiveOnlineTV.apk

Detection ratio: 17 / 53

Analysis date: 2016-01-14 02:54:18 UTC (1 week, 4 days ago)

0 0

Analysis | File detail | Additional information | Comments 0 | Votes | Behavioural information

Antivirus	Result	Update
AhnLab-V3	Android-PUP/Airpush.de57	20160115
Alibaba	A.L.Pri.optOut	20160115
Antiy-AVL	Trojan/AndroidOS.TSGeneric	20160115
Avira	ANDROID/ANDR.AirPush.MR.Gen	20160115
Baidu-International	PUA.Android.AirPush.M	20160115
CAT-QuickHeal	Android.Airpush.G (AdWare)	20160115
Cyren	AndroidOS/GenPua.686C40C8!Olympus	20160115
DrWeb	Adware.Airpush.24.origin	20160115
ESET-NOD32	a variant of Android/AdDisplay.AirPush.I potentially unwanted	20160115
Fortinet	Adware/AirPush!Android	20160115
Ikarus	PUA.AndroidOS.AirPush	20160115
McAfee	Artemis!686C40C8B03D	20160115
McAfee-GW-Edition	Artemis!686C40C8B03D	20160115
NANO-Antivirus	Trojan.Android.Airpush.dgiyls	20160115
Qihoo-360	Adware.Android.Gen	20160115
Sophos	Android Airpush (PUA)	20160115
Tencent	Android.Trojan.Andr.Wpaa	20160115

Link Hijacking

Summary

Data Collection

- **Collected 5,685** aggregator domains.
- **Inspected 1 TB traffic** to identify **309** channel providers.

Operational Insights

- **25%** of live streams originates from the servers hosted in Belize.
- **60% of analyzed streams** originates from the media servers provided by only **5 companies located in Belize, Switzerland, the Netherlands, Sweden, and Canada.**

Possible Infringements

- **64%** of parties providing media streams have been reported at least once for violating the copyrights of content owners.
- **5-7%** FLIS pages leverage trademark names and logos of popular TV channels and sports organizations to attract more visitors.

Substandard Advertisement

- **93%** of the video players on FLIS webpages were stuffed with overlay ads, hiding more than **80%** area of the player.
- FLIS services employ **deceptive techniques** to collect unintended clicks from visitors, leading visitors to open advertisement websites.

Illicit Monetization

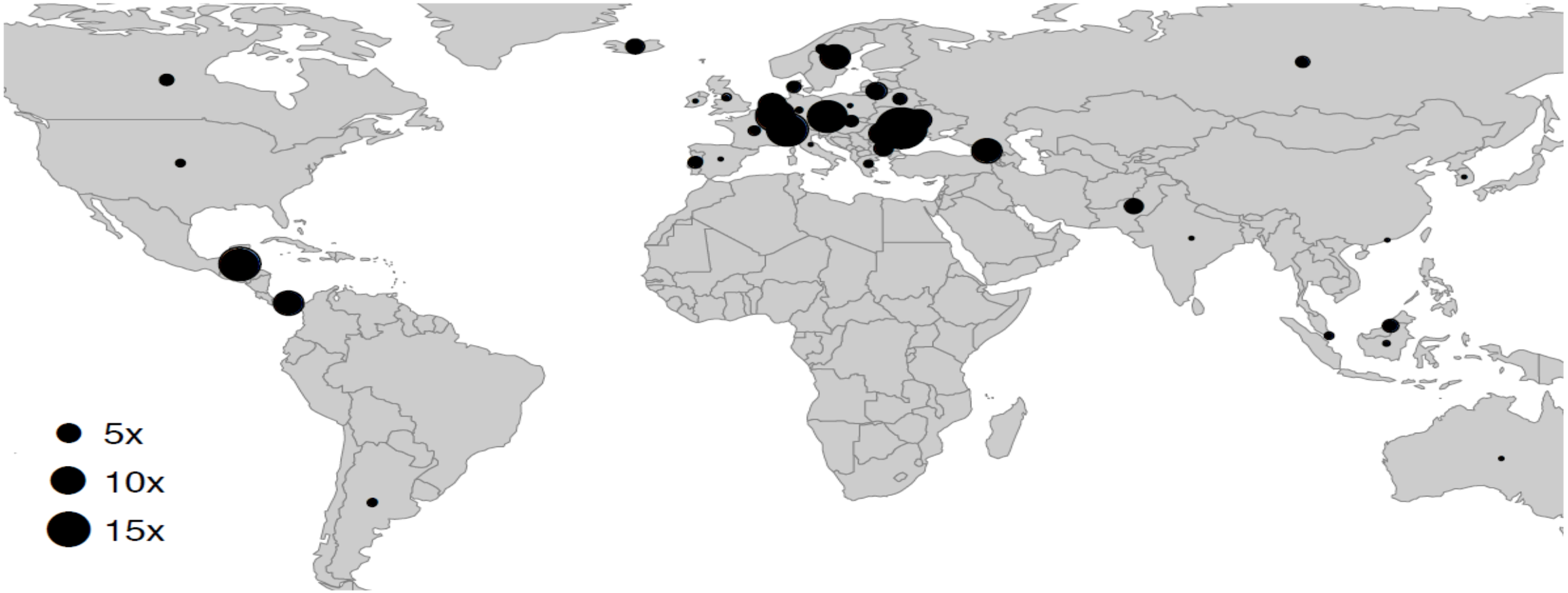
- **50% of ad-related websites were** malicious in nature, offering **malware, malicious browser extensions, and all sorts of scam pages.**
- Some FLIS services are also directly involved in **malware distribution via an Android application.**

Conclusion

- First empirical study of free live streaming services
- Developed an infrastructure that enabled
  - Mapping of the FLIS ecosystem
  - Automatic identification of the parties that index links of unauthorized free live streams and facilitate anonymous broadcast of live streams
- FLIS parties are often reported for copyright violations and host their infrastructure predominantly in Europe and Belize
- FLIS services are inclined towards intrusive and malicious monetization schemes at the expense of user security
    - Make heavy use of substandard and deceptive overlay advertisements
    - Leads the users to install malware binaries, malicious browser extensions, and fraudulent scams

Questions?

Aggregator Hosting Location



Relative distribution of the geographical location for aggregator websites. The size of each dot indicates the number of times a country is more prevalent in the distribution of aggregator websites compared to the distribution of the top 100,000 websites.

Redirection Chains Leading to Domains Offering Malicious Browser Extensions