Open Streaming Relays and the development of a Criminal Streaming Underworld

Marshall Eubanks

IETF-77 IEPG

March, 2010

Why am I here ?

- I (among other things) run AmericaFree.TV, an Internet Television network.
- We broadcasts multiple channels of high quality video content, specializing in Music Videos and long form content (i.e. movies and “regular” TV shows).
- I want to report on something we stumbled across.

It all started with a letter…

Americafree.tv
Designated Copyright Agent

Oct 28, 2009

Subject: DMCA Notice

1. I am the owner, or an agent authorized to act on behalf of the owner, of certain intellectual property rights. The intellectual property rights include the copyright in and the rights to distribute and broadcast live cricket matches relating to the Australia in India ODI Series 2009.

2. I would like to bring to your notice multiple copyright infringements occurring on your website and using your services related to rebroadcast of live cricket matches of the Australia in India ODI Series 2009 Match where Willow.Tv is the owner of these rights.

3. I may be contacted via email at legal@willow.tv, via phone on +91 9886540504 or at Syed Ansar, Willow TV India Pvt. Ltd.,203, Raheja plaza Commissiariat Road Bangalore 560 025 INDIA in relation to this notice.

4. The following channel on your website is broadcasting copyrighted live cricket via illegal rebroadcast of the broadcast feed::

rtmp://dvorak.americafree.tv/americafree&autostart=true&displayclick=fullscreen&stretching=exactfit

http://footheats1.blogspot.com/2009/09/channel-3.html

5. The feed described above sells, offers for sale, or makes available goods and/or services that infringe our intellectual property rights displaying Internet video streams of live cricket matches for which Willow.tv is the owner. I have a good faith belief that Americafree.tv Internet Services, Inc. are being used for infringing services. I understand that this notice may lead to the termination of the user account associated with the above stream.

6. I have a good faith belief that the copyright owner, its agent, or the law as described above does not authorize use of the copyrighted materials.

7. I swear, under penalty of perjury, that the information in the notification is accurate and that I am the copyright owner or am authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Truthfully,

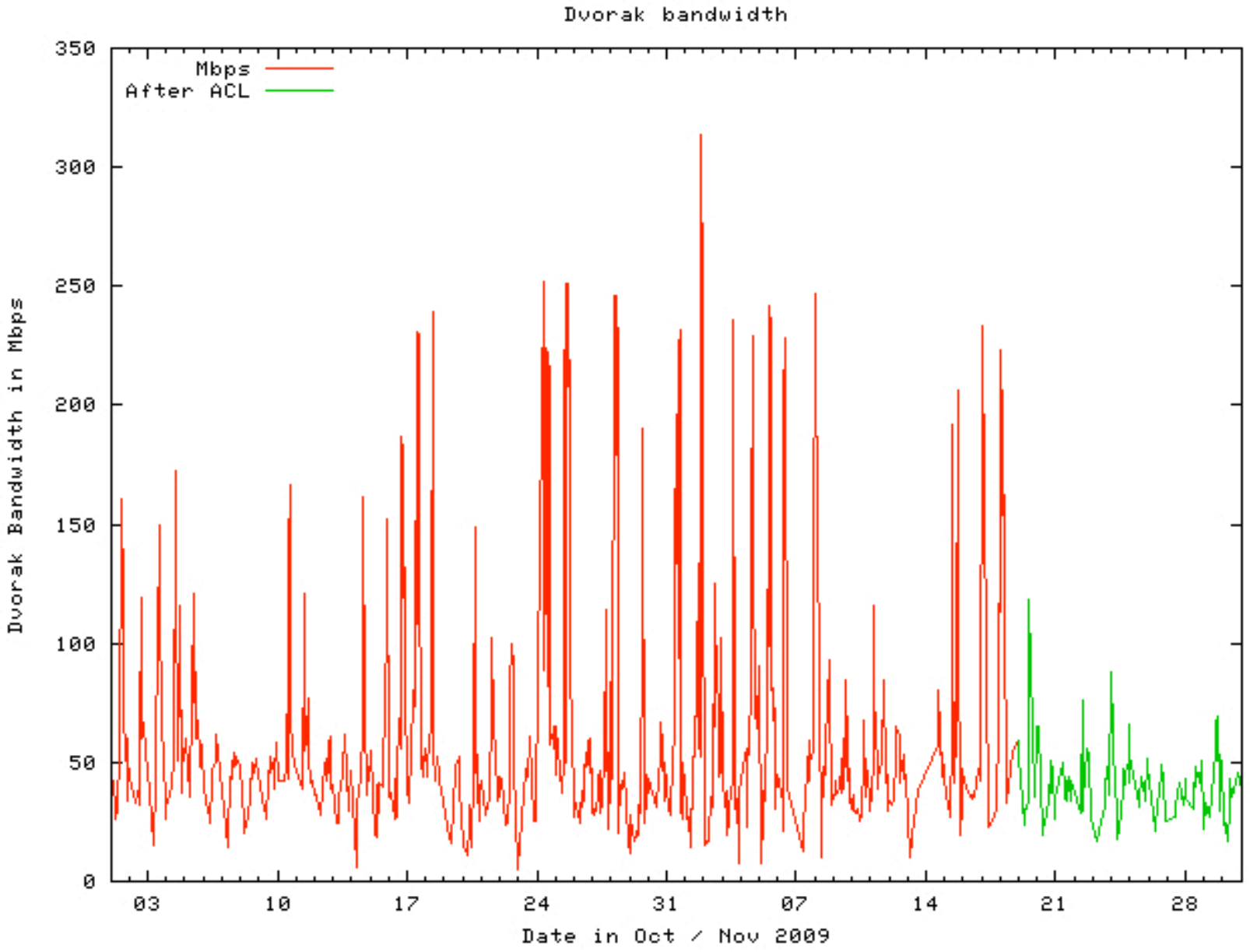
Syed Ansar

Willow TV, Inc.

Say What ?

- While we do not like to receive DMCA take down notices, the original response was… bemusement.
  - We don't have ***any*** Cricket video. Not even a frame.
  - We have licenses for all non public-domain material.
  - No one knew what Willow TV was talking about.
- But, still, attention must be paid, so we looked into it. Especially as we kept getting more letters.
  - ~ 1 per day
- Then I heard that there had been some unusual traffic patterns with the Dvorak server.
  - Uh oh…

Dvorak under attack



So, what's causing these 300 mbps traffic spikes ?

- First, this box (a Flash Media Server or FMS) was maxing out during the peaks.
  - This was an ***excellent*** load test for this box.
- Second, this traffic was mostly in the middle of the (US) night, a quiet time for us.
- Third, the logs had references to content names we don't use.
- Uh oh.

What is topcric.blogspot.com ?

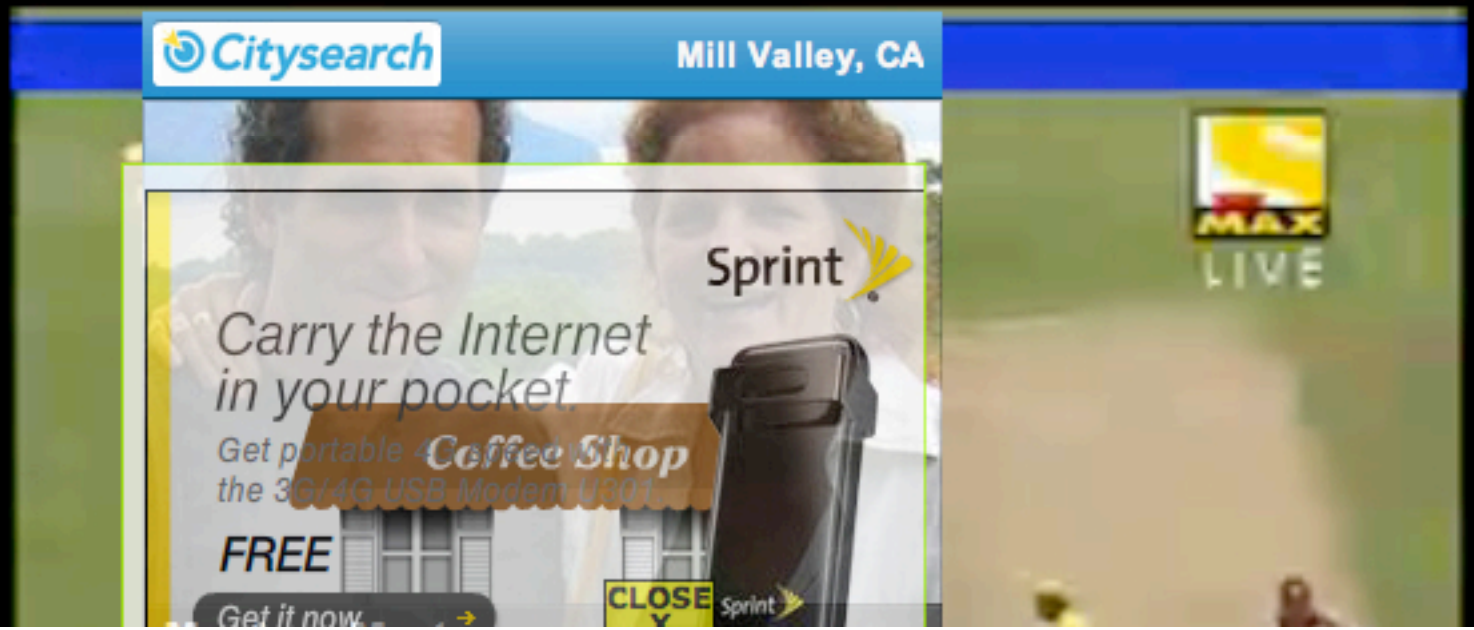
- I started looked at this from the ***other*** end.
- Most (but not all) of the letters referenced topcric.blogspot.com .
- What is that ?

Welcome to the Home of Live Cricket. Watch All Cric

Deccan Chargers v Delhi Daredevils Finisl

Chennai Super Kings v Kings XI Punjab LIV

Please Check all Channels to find best for y



Well, it ***looks*** professional

- This site looks professional, and even has ads (pop up, on screen, etc.) from Google etc.
- It is carrying a live Indian TV broadcast channel.
- As far as I can tell, this is totally pirated.
- It has 10 “channels” each of which (appears to be) a pirated server relay. Poor Dvorak was one of them. (The mix changes regularly.)
- Oh, and go there at your own risk, as it seems to be trying to insert something into windows machines.

What are they doing ?

- The channels point to something like
  - http://31indvsrl.webs.com/channel%201.html
- Which have in them something like

```
document.write(unescape('%0A%3C%65%6D%62%65%64%20%77%69%64%74%68%3D%22%36%30%30%22
    %20%68%65%69%67%68%74%3D%22%34%32%35%22%20%77%6D%6F%64%65%3D%22%6F%70%61%71%75%
    65%22%20%61%6C%6C%6F%77%66%75%6C%6C%73%63%72%65%65%6E%3D%22%74%72%75%65%22%20%7
    4%79%70%65%3D%22%61%70%70%6C%69%63%61%74%69%6F%6E%2F%78%2D%73%68%6F%63%6B%77%61
    %76%65%2D%66%6C%61%73%68%22%20%73%72%63%3D%22%68%74%74%70%3A%2F%2F%73%74%61%74%
    69%63%2E%62%61%6D%62%75%73%65%72%2E%63%6F%6D%2F%72%2F%70%6C%61%79%65%72%2E%73%7
    7%66%3F%75%73%65%72%6E%61%6D%65%3D%4C%61%6E%6B%61%63%72%69%63%6B%65%74%74%76%22
    %20%6E%61%6D%65%3D%22%62%70%6C%61%79%65%72%22%2F%3E%3C%61%20%68%72%65%66%3D%22%
    68%74%74%70%3A%2F%2F%63%72%69%6B%74%76%2E%62%6C%6F%67%73%70%6F%74%2E%63%6F%6D%2
    F%22%20%74%61%72%67%65%74%3D%22%5F%74%6F%70%22%3E%3C%69%6D%67%20%77%69%64%74%68
    %3D%22%32%34%38%22%20%68%65%69%67%68%74%3D%27%35%30%22%27%20%62%6F%72%64%65%72%
    3D%22%30%22%20%73%72%63%3D%22%68%74%74%70%3A%2F%2F%69%33%36%2E%74%69%6E%79%70%6
    9%63%2E%63%6F%6D%2F%32%71%6B%71%77%72%6B%2E%6A%70%67%22%20%61%6C%74%3D%22%22%20
    %73%74%79%6C%65%3D%22%6C%65%66%74%3A%20%33%33%35%70%78%3B%20%70%6F%73%69%74%69%
    6F%6E%3A%20%61%62%73%6F%6C%75%74%65%3B%20%74%6F%70%3A%20%33%35%30%70%78%3B%20%7
    7%69%64%74%68%3A%20%32%31%30%70%78%3B%22%2F%3E%3C%2F%61%3E'));
```

Digging Deeper

- If you unescape this, you get
  - `<embed width="600" height="425" wmode="opaque" allowfullscreen="true" type="application/x-shockwave-flash" src="http://static.bambuser.com/r/player.swf?username=Lankacricketty" name="bplayer"/>`
- To translate this, a FMS by the name of http://static.bambuser.com/r/ is being used by the pirates to serve a "file" (really a stream mount point) player.swf and a user name Lankacricketty. This then becomes (in this case) “Channel 10” of the pirate site.
- Now, maybe Bamuser is cool with this. We are not.
  - I apologize for using another victim, but somehow we managed to not save any of the code using us.

Why are there open streaming relays ?

- This is used a lot.
  - One server serves content to a bunch of secondary servers which face the public.
  - In webcasting sports, concerts, etc., one server serves through limited bandwidth at the venue to a server back at HQ, which replicates.
- What is scary is that there seems to be no means of apply a white list at any streaming server I know of.
  - If you are open, you are open to all.
  - IMHO, too many cycles spent on DRM and not enough on security.
  - IMHO, DRM is value subtracting.

Why is this scary ?

- Let's see. One pirate, one event, and one of my servers was maxed out.
  - 300 Mbps x 10 = 3 Gbps stolen ***for this event***.
  - But, guess what, most servers have higher limits. This server points to a Gig-E to the Internet. They could be stealing more than 300 Mbps per victim server. I don't know. I would guess 5 Gbps per event.
- This looks like a criminal enterprise to me. The code looks professional. They rotate the victim servers in and out. They know what they are doing.
- I wouldn't be surprised if in aggregate 100's of Gbps are being stolen in this fashion. If not, they will be.

What did we do ?

- Well, we don't generally need to accept an outside relay. If we do, we know who they are.
- So, I wrote code to
  - Look for incoming video streams.
  - Find the IP address of the host.
  - ACL that address if it is bogus.
- From January 23 to now, this has stopped 85 attacks, about 1.5 / day.
  - These came from 46 IP addresses, from all over.
  - Presumably these are all zombies.
- I also posted this to NANOG.

Conclusions

- Do not ignore letters from Indian lawyers. They may have technical significance.
- There are fairly professional criminals out there who are stealing bandwidth.
- There may be “root kits” to do this.
  - (Of course, these attacks do not have root access)
- They are hunting down media servers for victims.
  - FMS, Wowza and WMS at least appear to be vulnerable.
- The media server writers need to get on the stick and protect against this. ISPs hosting media servers should start looking at their traffic logs.