GUEST AUTHOR

The Sky is Falling

Could OTT From Unexpected Places Herald The End Of Television As We Know It?

Jack Burton
Principal
Broadband Success Partners
jburton@broadbandsuccess.com

Jack is a principal of Broadband Success Partners, a consultancy focused on helping service providers and their suppliers address their technology, product and marketing needs. Previously Jack was Senior Director of Systems Engineering for Altice USA and Cablevision Systems. With over 35 years of industry experience, Jack has also worked at MTV Networks, Tribune/United, and Warner/Amex. Jack has a BS in Electrical Engineering, from Rensselaer Polytechnic Institute.

There are many who say television is experiencing its second "Golden Age." More content is available than ever before, from a growing list of sources.

Old television programs and movies are also available. Many networks and studios have put their libraries of television online through both their own services and those of third parties, such as Netflix and Hulu.

Live television in digital form can be received over the air and through cable and satellite from stations and networks around the world. Some of these sources stream their content on the Internet themselves.

All of this material, live and recorded, is at risk of being streamed by third parties without consent.

VIDEO PIRACY THEN

In earlier days of video piracy, an "illegal box" was obtained through unscrupulous and possibly illegal methods. Many of the boxes were stolen goods themselves — originating from legitimate cable company sources and then modified to receive programming without proper authorization. Sometimes employees of the cable company would help (such as with the title character of Jim Carrey's "The Cable Guy").

Better security efforts by cable operators reduced these forms of theft to a trickle.

Bootleg videotapes and DVDs of Hollywood movies could be found being sold in the back of the barber shop or delicatessen. Just as with the legitimate video stores they once challenged, these sources, too, have gone away in favor of online streaming.

VIDEO PIRACY TODAY

The ease with which users can avail themselves of unauthorized content makes today's problem different from the use of illegal boxes of the past.

Let's look at the details:

No VSP Subscription Required

To stream video, a customer does not require a video services provider subscription from their Internet service provider. They only require an Internet connection. In fact, their Internet service provider might not even sell video services.

Generic Hardware

The hardware used to receive and display a video stream on a television screen is widely available from a variety of retail sources. Many of these same devices are used by legitimate streaming services. Streaming players are very inexpensive; a teenager could afford one after a night of babysitting.

Easy Adaptation

The generic hardware can be modified to receive illegal streams by installation of software. There is nothing inherently illegal about this software or the process of installing it.

The installation process is so easy that a purchaser of the generic hardware could follow instructions available on the Internet to install the software themselves, or go through a third-party agent to perform the modifications for them.

SHUTTERSTOCK.COM

Streaming Network Ecosystem

An entire global network of streaming sources and servers has evolved. These services collect and catalog streams or material from a variety of sources and make them available for others to receive or re-stream. This makes tracing the source of an illegitimate stream difficult. Many services are available for re-sale by brokers or middlemen, making it more difficult to track down customers should one establishment become compromised.

In the course of preparing this article, I found it nearly impossible to tell an online store of a legitimate live stream seller from an illegitimate one.

Cottage Industry

The third-party agents involved in installing the new software can also install the appropriate links to purveyors of unauthorized content. They can then act as agents of those parties and provide end users with subscriptions to streaming services from those services or their re-streaming partners.

OTHER STREAMING VIDEO SERVICES

There are many large companies offering completely legitimate streaming services, such as Netflix, HBO, Sling TV, Hulu, Amazon, CBS, etc. There are also smaller legitimate sources of free material such as Crackle, Viewster, PlutoTV, and SnagFilms. Some customers could start out intending to "go legit," buy the required hardware and subscriptions, and downgrade their cable service to broadcast basic or Internet only.

These same customers could take the same hardware, download a few bits of software, and enter the world of unauthorized streaming. They can then stop their subscriptions to the above-mentioned services and continue to watch the same (and often much more) programming.

EDITORIAL CREDIT: DENNIZN / SHUTTERSTOCK.COM

Amazon Fire TV Stick is one of many legitimate consumer-friendly streaming devices.

There are many less than legitimate program aggregation sources, each with their own software to load on the player hardware. Some have an advanced user interface rivaling the best legitimate services.

It would be difficult for the end user to know which are legitimate services and which are not.

STREAM SOURCES — OUR OBSERVATIONS

Live streams from various cable and broadcast networks we observed for several months generally had IP addresses that originate from Europe, irrespective of whether the source channel is an American, Canadian, or European service. Recently, the European source used by many live streaming aggregators was blocked or shut down, and the streams re-appeared from a stateside IP address in less than 24 hours. Streams of unauthorized recorded content are available from many different sources, usually including Eastern Europe, the Middle East, and various island nations. The unauthorized recordings may have been received from a programming service, authorized streaming service, DVD, over the air, or even shot with a camera in a movie theater. Many recorded TV shows and movies carry the logo bugs of the service that transmitted them.

Of course, an American live stream is not really originating in Europe. Someone in the U.S. is receiving the stream and sending it to Europe for re-streaming.

This can be confirmed from the locally inserted commercials, set-top box artifacts, or emergency alert broadcasts.

WHO IS DOING IT, AND IS IT LEGAL?

In a social media forum, I came across a person acting as a player in the cottage industry just described. He was responding to complaints about their cable service. He offered people an alternative: Buy a streaming player and send it to him, pay a little cash, and get back something that can get all of your TV from before and more. You can then disconnect your cable video service and save lots of money.

Of course, some were a bit leery about the legality of doing such a thing and posted their concerns. He would respond that lawyers, policemen, fire fighters, and other upstanding community members were customers, and that the current law does not define end-user streaming as illegal. He is doing dozens of these conversions every month, and has many happy "customers."

While it may be true that under current law end-customers face a limited risk of committing a crime, the subscription seller and software loader is almost certainly doing so under the "Inducement Rule," which was used in the Napster days to go after those selling means to violate copyright law. The inducement rule basically states that one promoting or enabling copyright violation is committing such a violation.

What about the streaming sites? Obviously, having copyrighted material on a server and broadcasting it without authorization is a direct violation. Copyright violations contained within the material advertising unauthorized streams may be used as indications of wider violations of copyright to assist in legal challenges against these services.

It is clear that we need better legal and technological tools to address this problem.

PAGE 48 ▶

WHAT TO DO?

With the problem defined, what can be done to combat this threat?

Legislate/Litigate

At a minimum, the existing protections provided by the DMCA must be extended to specifically cover unauthorized streaming. This type of change has already happened in Europe by court interpretation. New legislation at the national level should make it clear that *stealing is stealing, and receiving stolen goods (or TV services) is a crime.*

Those providing any of the unauthorized parts of the ecosystem could be challenged in civil court. Once identified, a streaming server provider or box modifier could be sued for loss of revenue or other damages. End users could similarly be targeted.

Public Relations

Faced with losses from illegal music downloading, the music industry ultimately reached a model of distribution based on inexpensive authorized downloads combined with free or inexpensive authorized streaming subscription sources. They also waged a public relations campaign designed to make it clear what was legal and what was not. Efforts started by the Alliance For Creativity, for example, help to educate the public about the ultimate costs of unauthorized streaming. Internal industry efforts are also underway at NCTA and CTAM. New campaigns could be undertaken to emphasize the risks to the end user, outlined below, and to help the public determine the difference between a legitimate streaming provider and an unauthorized one.

The home user of unauthorized streaming services faces several risks:

Legal Action

When effective laws can be enforced, the users risk criminal or civil action. They might be traced technologically or from a subscriber list of an unauthorized streaming service to which they subscribed.

Downloading of malware could jeopardize the security of their home network and all devices connected to it

The software required to play unauthorized streams and catalog the unauthorized products can have hidden malicious programs embedded within them. Software tools required to install the player software products to a streaming device from a PC are even more at risk. Malware could range from password-stealing trojans to ransomware and spam generators. With the software installed on a device behind a user's router, other devices in the home network can be targeted.

Unreliable service as streams and their providers come and go

As unauthorized stream sources are taken down, the user will lose service. We observed that sources may not operate on a regular basis even under normal circumstances. Once a source is lost, the user may need to take direct action to find a new way to obtain a replacement, including loading a new player or specifying new access credentials.

As stated previously, the end user may be completely unaware that their choice of streaming service provider is selling unauthorized streams.

TECHNOLOGY

On the player front, one could mandate hardware protection (as with the HDMI interface copy protection scheme) but it would take years to end up in the products, and unprotected products or hacks would likely still be available.

Why not go after the illegal streaming servers? Internet service providers have the means to detect and determine the IP address source of illegal streams, once they have been identified as such. Those IP addresses could be traced back to their ISP and ultimately to the source server via the same means used to locate filesharing servers. This would mean that the content owners and ISPs would have to cooperate, or at least respond to court ordered requests, as they do with filesharing today.

Watermarking technology provides a good basis on which to build a means to identify streams. If all legitimate streams are uniquely marked at as many points in the distribution chain as possible, a peek into the watermark in the unauthorized stream could point to the source or at least the video service provider involved. The same techniques could be used to tag VOD streams as their authorized originals are transferred into an unauthorized streaming source library.

Encryption

If the stream user employs a VPN, the source address of the streaming server is encapsulated in the encrypted stream. If the user's ISP blocks that address, the stream will still go through as an encrypted flow from the source IP of the VPN service providing the encryption to the user rather than the streaming server itself. For this reason, the only truly effective means to stopping the stream would have to be employed at the ISP of the server rather than just the user.

Blocking streams involves network neutrality considerations. Most network neutrality laws and regulations allow for blocking "illegal" transmissions — all the more reason to make certain that laws define unauthorized streams as illegal.

SUMMARY

The plethora of streaming hardware, coupled with widespread availability of unauthorized sources of aggregation and streaming content is a growing phenomenon which, if unchecked, will become larger and larger. The "cottage industry" could grow bolder, selling subscriptions and "loaded" boxes at retail outlets. Streaming video from unauthorized sources represents a challenge to the very existence of the television industry.

Programmers and service providers must come together to step up to the challenge. Only programmers can help to make their authorized streams more identifiable, and only service providers can trace those streams to their unauthorized sources and hopefully stop them. The actions we, as an industry, take now will help determine if television's new Golden Age turns out to be "Fool's Gold."

This piece reflects the opinions of Jack Burton and Broadband Success Partners, and does not necessarily reflect the views of this publication.