Illegal Streaming and Cyber Security Risks:

A dangerous status quo?

AISP Working Paper, Autumn 2014

AISP

Association of Internet Security Professionals

EXECUTIVE SUMMARY

Online video consumption has risen massively over the years, with the OECD estimating that video will exceed 91% of global consumer Internet traffic by the end of 2014. Alongside this enormous quantity of mostly user-generated content an equally massive black market has developed, where TV shows, films and live sports are streamed with little regard for copyright law. While debates over illegal streaming are often cast as battles between the interests of wealthy broadcasting industry executives and lobbyists on the one hand and those of freedom of speech activists and internet entrepreneurs on the other, this ought not be the case. The cyber security dangers that accessing unauthorized videos pose to individual computers mean that **illegal streaming can be as damaging to the user as it is to the copyright holders** of our most cherished sports, television and film content.

While copyright law can be complex and somewhat contradictory (due especially to the recently aborted attempts to push through comprehensive legislation), it is clear that streaming sites offering video content for which the provider does not own any rights undermine the basic notion of copyright as set out in the U.S. Constitution. Copyright exists to encourage new creations yet many are now arguing that such laws impede online innovation. Such arguments are misguided, however, for weakening intellectual property rights would be a blow to any entrepreneur looking to carve out a space for his or her business, and for any artist who seeks to live off his or her creations.

Much space has already been dedicated to the impact of illegal streaming on the film and television industries, but live-streaming sports events is emerging as a crucial battleground between copyright holders and internet pirates. A continual escalation in broadcasters' bidding wars for sports rights coupled with technological developments have driven more viewers than ever to illegal streaming for their sports intake. It is inevitable that this decrease in sports' legal viewership takes a toll on both the quality of the sporting events and reinvestment in the future of sports leagues.

The greatest, and most often neglected, cost of illegal streaming, however, falls on the user. Not only will individual consumers suffer from a lack of reinvestment in the content they love, but illegal streaming opens the door to a host of cyber security dangers. From *botnets* to DDoS attacks, **video streaming has become the number one method to propagate highly dangerous malware on the Internet**. As this paper argues, stymieing the hacking wave that has taken off in recent years entails mounting awareness campaigns targeted at computer users everywhere, informing individuals of the personal risks that illegal streaming exposes them to.

Finally, this paper sets out a series of recommendations for the future, including increasing international cooperation, further awareness campaigns on the risks of illegal streaming for individual users, and a clearer and more consistent legal approach to online copyright infringement.

INTRODUCTION

Traditionally perceived as one of the most resilient staples of modern Internet culture, this favorite bandwidth-guzzling pastime has in fact a long history behind it. The basic mechanism that underpins streaming was patented in the 1920s by George O. Squier, a major general in the U.S. Army. His company, Wired Radio (later rebranded to Muzak Inc.), sought to find more efficient ways to transmit information over wires – atechnology

they called **telephone carrier multiplexing**[1]. Adapted from the fledgling radio technology, his company used this invention to pipe background music to various businesses, such as shops and elevators.

With the advent of the digital age, it wasn't long until that technology managed to catch up and surpass the requirements for online streaming. The first experiments with live video streaming can be found in the early 1990s. *Severe Tire Damage* was the first band to perform live on the Internet in 1993, followed by the 1995 first live transmission of a sports event, a baseball match between the New York Yankees and the Seattle Mariners[2].

These first experiments involved professional-grade hardware equipment that far surpassed the possibilities of early Internet surfers. It wasn't until the early 2000s, with the rise of the Flash video technology that online streaming actually took off, reaching a mass audience.

Online video consumption has risen massively over the years, with the OECD estimating that by the end of 2014 video will exceed 91% of global consumer Internet traffic[3]. This trend is fueled on one hand by user-generated content (UGC) and on the other by video-on-demand and live streaming services. Generally paid, the latter category has given birth to an equally massive **black market**, which offers the same services for free, therefore digitally infringing on copyright laws. According to the OECD, this type of digital piracy, called **illegal video streaming,** has grown rapidly due to its low production and delivery costs and advances in technology that has increased access to source material[4]. Moreover, the OECD report shows that users routinely fail to see digital piracy as un-ethical and are generally unaware of the security problems associated with accessing illegal video content.

Generally framed as a battle fought between copyright holders and users, between a money-grubbing industry and the Internet's prevalent free to use culture, this report will argue that in reality illegal streaming poses numerous risks to the consumer. Indeed, in our research we found that a major assumption among illegal streamers is that 'they deserve access to free content' or that doing so 'does no harm'. Such claims are easily refuted upon closer inspection.

In reality, accessing black market streaming services is the fastest growing propagation method for malware, giving both established groups (such as Anonymous or LulzSec) and wannabe hackers the technical and financial means to carry out their agendas. Illegal video streaming has thus become one of the main enablers of **cybercrime**.

1 Mischa Schwartz, "Origins of Carrier Multiplexing – Major George Owen Squier and AT&T", Columbia University
2 Neil Strauss, "Rolling Stones Live on Internet ; Both a Big Deal and a Little Deal", The New York Times, November 22, 1994
3 Marc Latouche, "The Economics of Personal Data and Privacy", OECD, 2007
*4 ***OECD Report, "Piracy of Digital Content", 2009, pp. 5-7*

I. WHAT IS COPYRIGHT AND WHY DO WE NEED IT?

Copyright refers to a set of exclusive rights that come into existence when an original work is created, performed or published. In the United States, copyright is enshrined in Article 1, Section 8, Clause 8 of the Constitution: "To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries". The idea behind this Clause is that creation and innovation in the arts and sciences ultimately benefits the general public and thus should be encouraged. For the Founders as for today's public authorities, the best way to encourage creation is to grant creators with the exclusive rights to their creations, which they are then free to waive or sell (to new *copyright holders*) as they choose.

These rights give creators the chance to financially benefit from their creations, which should encourage them to continue creating and innovating. Few would question that new creations benefit the general public. From technological developments to creative masterpieces, creators regularly impact the individual's experience for the better. Moreover, copyright applies only for a limited time period, after which creations fall into the public domain (though when exactly this occurs depends on a number of factors[5]). Therefore, while the price of accessing a copyrighted work may impede its accessibility for certain members of the public, creations can be enjoyed more or less universally after a certain period of time.

Copyright is also designed to protect larger economic concerns. As the Internet Policy Task Force's (IPTF) 2013 Green Paper on Copyright Policy points out[6], "copyright-intensive industries contributed 5.1 million jobs and grew by 46.3 percent between 1990 and 2011, outpacing other IP- [intellectual property] intensive industries as well [as] non-IP-intensive ones". Indeed, industries that rely on copyright law contributed 4.4 percent of U.S. GDP in 2010, or approximately $641 billion.

Since 1978, copyright has been automatic, meaning that creators do not need to register their works with the Copyright Office in order to retain their rights. Neither do copyright holders need to place a copyright symbol (©) after on their works if they belong to a member state of the 1989 Berne Convention for the Protection of Literary and Artistic Works.

As researchers at the University of Texas set out[7], copyright relates to four key activities: reproduction, derivative works, public performance and public display. First, no one other than the copyright holder may authorize the reproduction and distribution/publication of their works. Second, any creation based on or containing copyrighted elements of an existing work must be approved by the copyright holder of the former. Third, public performances of a copyrighted work must be authorized by the creator and/or copyright holder. The same goes for a public display of the work.

These activities are important to bear in mind when approaching online streaming.

Copyright legislation and streaming

While the rules of copyright were written with the understanding that future technologies would transform the way original works, whether scientific or artistic, are consumed, it is safe to say that the Internet has disrupted the world to an unprecedented extent. As the IPTF puts it, "Never before has it been possible for individuals to create and disseminate multiple perfect copies of works virtually instantaneously and essentially cost-free." This reproductive and distributive capacity has clear implications for copyright law.

5 *Lolly Gasaway, "When U.S. Works Pass Into the Public Domain", University of North Carolina, April 11, 2003. Available at http://www.unc.edu/~unclng/public-d.htm*
6 **** Department of Commerce, Internet Policy Task Force, "Copyright Policy, Creativity and Innovation in the Digital Economy", July 2013*
7 **** University of Texas, Austin School of Informatics "What is Copyright ?" in INF 335 Copyright Module, Available on https://cyberspace.ischool.utexas.edu/course/copyright/2.php*

The development of the Internet has meant the pace of technological change is increasing at an unprecedented rate, making it harder and harder for legislation and case law to keep up. For some[8], the solution to this problem is to avoid applying copyright law to the Internet as far as possible, the idea being that attempts to enforce copyright regulation will obstruct online innovation. For governments, the challenge lies in finding the "sweet spot", as former U.S. Secretary of Commerce Gary Locke once referred to it – where policy protects creators' rights without hampering creativity and the free flow of information.

For streaming, the key piece of legislation is the 1976 Copyright Act, which remains the primary basis of copyright law in the United States. The (in)famous 'Transmit Clause'[9] of the Act grants the copyright holder the exclusive right "to transmit or otherwise communicate a performance or display of work… to the public, by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times". Developed following the advent of cable TV, where "community antenna systems" were transmitting cable signals to deliver content they did not own to paying customers, the Transmit Clause was clearly written with a view towards the unknown future, including "any device or process" within its scope".

Today, illegal streaming works in a similar manner to the community antenna systems of the 1970s. Content that is broadcast by copyright holders on television or other platforms is subsequently recorded and uploaded for users to stream on a multitude of third party sites. Crucial to the legality of this kind of streaming (where no royalties are paid to copyright holders) is the question of whether the distribution of content constitutes a *public or private performance*. According to the U.S. Code (17 § 101), a public performance means:

> ***(1)*** *to perform or display it at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered; or*
>
> ***(2)*** *to transmit or otherwise communicate a performance or display of the work to a place specified by clause (1) or to the public, by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times.*

While the above definition makes it clear that unauthorized streaming falls into the category of public performance and thus runs counter to the law, some have maintained that streaming constitutes a private performance by virtue of its individualized format. In the Second Circuit's decision in WNET vs. Aereo, the latter a New York company that allowed users to stream live and time-shifted television broadcasts through online devices, the Court held that separate recordings of broadcasts did not constitute additional public performances. "Each transmission of a program could be received by only one […] customer, namely the customer who requested that the copy be created. No other […] customer could receive a transmission generated from that particular copy", the ruling stated[10].

However, this ruling seems to stem from a misunderstanding of how streaming works. As Jon Garon of Northern Kentucky University argues[11], "In actuality, every Internet distribution is uniquely identified to a particular individual […] Under this view, there would never be any performance and everything would be

8 http://rehman380.wordpress.com/, *Accessed on September 2, 2014*
9 **** Copyright Law of the United States of America, "Subject Matter and Scope of Copyright", Title 17 of the United States Code, Circular 92, Chapter 1.*
10 *WNET, Thirteen v. Aereo, Inc., 712 F.3d 676 (2d Cir. 2013)*
11 *Jon M. Garon, "Revisiting the Public Performance Right in the Battle over Broadcast", Business Law Today, November 7, 2013*

a distribution only." In other words, while streaming takes the form of many individual transfers rather than a mass broadcast, the results are similar.

In a June 2014 ruling on Aereo, the U.S. Supreme Court[12] agreed with the latter analysis, stating, "behind-the-scenes technological differences do not distinguish Aereo's system from cable systems, which do perform publicly."

In 2013, an interesting ruling came from the European Union's highest court, The European Court of Justice (ECJ), in a ruling involving the relationship between streaming and copyright law[13]. It ruled that websites that retransmit live TV on the Internet (IPTV), without license from broadcasters are in breach of copyright. The Court deemed that original broadcasters are "authors" of the programming aired, thus giving them exclusive right to restrict its use.

While the illegality of unauthorized streaming is clear, however, punishment is less consistent. While distributing a copyrighted work in the United States is classed as a felony, the penalty for streaming illegal content is a misdemeanor. The Stop Online Piracy Act (SOPA), brought before the House Judiciary Committee in November 2011, aimed to harmonize the penalties for distribution and streaming before it was suspended in 2012. The 2013 IPTF Green Paper, which also recommends harmonization, was viewed by many[14] as a sign that the White House wishes to bring SOPA or a similar Act back to Congress.

So far, governments generally use a 'notice and takedown' mechanism to combat illegal streaming, in which illegal content is identified and the hosting service notified that they must promptly remove such content. There are several problems with this method. First, the notice and takedown mechanism places the burden on the artist/copyright holder (the victim) to prevent pirated copies of their works from circulating. Second, the service hosting illegal content uploaded by users has little incentive to promptly comply with the copyright holder's notice, often making the latter jump through administrative hoops and putting off removing the content for as long as possible[15]. Another controversial SOPA prevision aimed to solve this second problem by allowing law enforcement to immediately block access to Internet domains infringing copyright law.

The third problem is the sheer scale of illegal content available to stream online, and it is to this issue that we shall now turn.

The scale of illegal streaming

For obvious reasons, it is difficult to get a clear picture of just how many individuals regularly illegally stream content online but the numbers we do have show that an immense level of pirated content exists.

As a 2013 study[16] from George Mason University points out, the Motion Picture Association of America (an association of 6 companies) sent over 13.2 million takedown notices to site operators over just the six-month period of March-August 2013. If six companies can identify 13.2 million illegal streaming files (to say nothing of files for which they do not own the rights) over six months, we can only imagine the true scale of illegal content being streamed online at any given time.

Earlier this year, Business Insider conducted an online survey on the scale of illegal streaming on a pool of 549 participants[17]. The results shed some light into the behavior and motivations of users that chose to

12 American Broadcasting Cos., Inc.,et al. v . Aereo, Inc., Fka Bamboom Labs, Inc., No.13-461 (Supreme Court of the United States, June 2014)
13 Case C-607/11, ITV v. TVCatchup, Judgment of 7 March 2013
14 Andrea Peterson, "SOPA Died in 2012, but Obama Administration Wants to Revive Part of It", The Washington Post, August 5, 2013
15 Lawrence J. Spiwak, "Doing Nothing Is Not an Option to Stop On-Line Piracy", The Hill, March 25, 2014
16 Bruce Boyden, "The Failre of the DMCA Notice and Takedown System", Center For the Protection of Intellectual Property, Geroge Mason University, December 2013
17 Christina Sterbenz, Andy Kiersz, Gus Lubin, "Here's How Many People Really Use Sketchy Streaming Sites – and Why", Business Insider, April 28, 2014

stream unlicensed content. Although a paltry 14% of respondents admitted to streaming such content, the scale of content available online leads to believe that some users of illegal services may have been reluctant to admit an activity that is illegal. 39% said they primarily stream TV series, 27% movies and a mere 10% opted for sports. The survey uncovered that 42% of respondents had been streaming for more than three years, proving that illegal streaming has become a staple of the modern Internet culture. Among the reasons they cited was the lack of availability on licensed streaming platforms of the content they desired - 55%-, while only 11% motivated their choice because they believed they shouldn't have to pay for the content. What was interesting though in Business Insider's findings is that 34% of respondents have no opinion on whether streaming unlicensed content should be illegal, pointing to a lack of awareness and interest among the general populace over this topic.

The latest battleground for illegal streaming is in the sports sector, which this report has chosen to dedicate an entire section to (see below). The 2014 FIFA World Cup shattered US online viewing records, becoming the most streamed live event[18] in the country's history. It has also been shown streaming were doing so illegally. According to the site Torrent Freak[19], some games garnered as many as 500,000 illegal streamers. During the 2014 Winter Olympics in Sochi, officials estimated that 98% of viewing took place through legal channels. Nonetheless, broadcast companies like NBC reportedly took down[20] "45,000 instances of illegally posted video or pirate streams" during the games.

Conclusions

As this chapter has tried to point out, U.S. corporate law is increasingly complex on the topic of streaming, legal or otherwise. Over the past 10 years, case law has grown in size, often with contradictory interpretations as to what constitutes infringing of copyright material. With comprehensive legislation scuttled and the incumbent administration yet undecided on the subject, it is our estimation that we are approaching a turning point in the history of copyright law. While we understand the importance of distributing artistic works to ever-larger audiences and the major importance of the Internet as main dissemination channel, this should not come at the expense of rights holders. Moreover, we have found no evidence that enforcing a fair legal online climate would stifle e-innovation. One must look no farther than the patent system, which has encouraged investment and the development of new ideas since it protects the holder's intellectual property. Therefore, we contend that the economic benefits of ensuring a healthy legal environment for creative artists and the associated business ecosystem needs to be upheld.

As this report will underscore in the forthcoming sections, illegal streaming represents marked risks for both consumers and various industries. To illustrate this, we shall now turn to the impact the distribution of unlicensed content has had on the sports industry and the worrying trend that can be envisaged if the status quo is left unchecked.

18 Shannon Bond, "World Cup Sets U.S. Live Streaming Record", Financial Times, July 2, 2014
19 *** "Millions Watch World Cup Through Pirated Live Streams", TorrentFreak, July 1, 2014
20 David Bauer, "NBC Says Thousands of Illegal Video Stopped", Associated Press, February 27, 2014

II. DIGITAL SPORTS PIRACY

The sale of broadcasting rights by sports teams and organizations has long been a central aspect of the sports industry's revenue. Over the years, broadcasters have been increasingly willing to pay hefty sums for the acquisition of exclusive rights for particular games and seasons. Various changes to the broadcasting industry, which allowed for the entry into the market of private Pay-TV firms, as well as various technological advances have significantly altered the landscape of the sports broadcasting industry.

However, the continued rise of digital sports piracy threatens both the broadcasting industry and sports organizations in terms of revenue and future investments and growth. Broadcasting companies spend significant funds on obtaining the exclusive rights to broadcast sports and ensure high quality and access to live coverage for their customers by continuously innovating. If the dangerous trend of sports piracy continues down its current path, the value of sports rights will decrease substantially, leaving broadcasters unwilling to pay the same price for these rights. As a result, sports revenues will diminish, leading to an overall negative impact on the sports industry in terms of investment and development. Not only is online sports piracy illegal, it also harms our wider economy by taking away revenue from legitimate broadcasters and sports organizations and placing it in the hands of pirates.

Broadcasting and sports – a brief history in Europe

The sale of broadcasting rights has traditionally been one of the largest sources of revenue for teams, sports organizations and leagues who are the owners of the rights. Over the last 15 years the industry has undergone several changes resulting in increased competition in the sports broadcasting industry and a rise in prices, with the effect of increased revenues for sports organizations. New technological advances have altered the way in which we view and appreciate sports and have created an incentive for the industry to evolve to meet the new digital demands of consumers.

The demand for sports rights

One of the main evolutions in the sports broadcasting industry in Europe has been a move away from public service broadcasting to bids for sports rights made by private Pay-TV firms, which begun to enter the market in the 1980s, in search of revenue from highly popular sporting events.[21]

Communication policy

Prior to the 1980's, the television sector was limited to public broadcasters with the exception of the US, Japan and Canada, which allowed private broadcasting companies access to the market much earlier and hence were dominated by competition in the post-war years.[22] In Europe, there were few players in the market as well as strict regulation of European broadcasting, which meant European channels were unable to pay the same amount for sports rights as their American counterparts. In the case of the BBC, the company's monopoly power meant it was able to obtain exclusive broadcasting rights for relatively cheap and even with the arrival of ITV on the scene (together they paid £2.6 million a year in 1983-85 to air live division one football league games).[23]

In the late 1980s, once governments began to relax their policy on television rights to allow for more options, the European broadcasting industry commercialized, creating an opportunity for the emergence of Pay-TV channels. In order to strengthen their market position these profit maximizing broadcasters began to bid significant sums to air live sports events

21 *Chris Gratton, and Harry Arne. Solberg. The Economics of Sports Broadcasting. (London: Routledge, 2007), 4.*
22 *Noll, Roger G. "Broadcasting and Team Sports". 06-16. Stanford: Stanford Institute for Economic Policy Research, (2007): 5.*
23 *Gratton and Solberg, Economics of Sports, 8.*

via cable satellite and terrestrial broadcasting.[24] The rise of commercial broadcasting and the increased number of players entering the market were largely responsible for the rise in demand for sports rights, the subsequent increase in price and an overall increase in the number of sporting events aired on television.[25]

Since public broadcasting companies like the BBC were funded predominately by taxpayers' money, they were inclined to air programs that would obtain mass approval by the public. Commercial broadcasters, on the other hand, were not bound by such obligations with their main aim being to maximize profits. While the BBC did air live sporting events, they could not dedicate too much of their programming to this cause as it would have been viewed as unbalanced for a public broadcasting company. As private broadcasting companies came to realize that the popularity of other shows and programs had declined, given the lack of need to watch these programs in real time, they soon began to understand the inelastic demand for live sports and the potential profits to be gained. This spurred many to begin to bid for high-profile sports rights contracts to increase audiences, subscriptions and advertising revenue. Given the wide audience reach of live sports programs and advertisers' interest in reaching these audiences, high profile sporting events such as the Premier League and NFL were particularly attractive due the revenue they bring about (broadcasters tend to charge more for advertising space during popular sporting games). The entry of new broadcasting companies into the market spurred an increase in the buyers of sports rights, competition and price, eventually leading to substantial rises in television income.

In addition, European private commercial broadcasters charge a subscribers fee for their channels, which also adds to the overall profit of airing a popular sporting event. Given these two profit-maximizing aspects, commercial and Pay-TV broadcasters have over the years been willing to pay increasingly more for sports rights, given that the size of the potential audience is large enough to attract advertising and an increase in subscriptions. The more sports channels and events a broadcaster is able to offer, the more willing consumers will be to pay for a subscription to these channels.

Difference between the US and Europe

There have been major differences between the US and European sports broadcasting industries in the post-war period. In Europe, sporting events were primarily broadcast on public service broadcasting channels until the 1980s. Today, Pay-TV channels have a greater slice of sports rights while restricting public channels to highlights. For example, live matches from the domestic premier leagues in the big-five European football nations (UK, Spain, Italy, Germany and France) are only screened on Pay-TV channels, which have continuously been able to outbid free-to-air broadcasters for exclusive sports rights.

In the US, free-to-air broadcasting is the dominant version for sports broadcasting. The predominant motive for bidding for the sports rights of MLB, NBA and NHL is the ability to sell advertising spaces for a considerably higher price than usual. Advertising breaks tend to last 3 times longer than those in Europe, which explains why, in Europe, broadcasters need additional revenue from subscribers.[26]

Overall, the changes in communication policy with regards to broadcasting companies in Europe, which resulted in an increase of entrants into the market, are responsible for the overall quantity of sports broadcasts and the increase in fees for sports rights.[27]

24 Gratton and Solberg, Economics of Sports, 8.
25 Noll, "Broadcasting and Team Sports", 6.
26 Gratton and Solberg, Economics of Sports, 4
27 Noll, "Broadcasting and Team Sports", 7

Technological change

The rise of new technologies and different delivery methods for broadcast companies have also been responsible for driving the demand and price of sports rights up. The increased desire of consumers to watch their preferred sports in digital form, such as on tablets, computers and smartphones, has encouraged the industry to innovate further. Pay-TV operators, telecommunications firms and free-to-air broadcasters have been encouraged to follow this consumer trend and increasingly provide live online viewing platforms for its customers. In 2013, Verizon recognized this trend and struck a deal with the NFL worth $1 billion for the rights to air a greater number of NFL games over smartphones.[28] Such technological revolution on the part of broadcasters and new players has resulted in an enhanced experience for the fan, with the additional reward of attracting a greater audience, that can now watch their live games online and on a variety of devices.

The new digital age that has made its way to the live sports industry will provide positive change for the broadcasting market overall, as 'sports have traditionally played a significant role in the development of new media technology and its adoption among consumers'.[29]

This remains a reason why the demand and price of sports broadcasting rights will continue to rise as broadcasters fight to obtain the latest new-media technology to host these live events online. Moreover, innovation will also be encouraged in this new environment. For example, Hutchins and Rowe (2009: 355-6) have argued that we may be moving to a new online model, one which is defined "by 'digital plenitude' with the internet significantly lowering entry barriers for media companies and sporting organizations to exploit sports content".[30]

28 Futterman, Matthew, and Spencer Ante. "Verizon Pads NFL Deal." Wall Street Journal. 4 June 2013.
29 Tom Evens, Petros Iosifidis and Paul Smith. The Political Economy of Television Sports Rights: Between Culture and Commerce (Palgrave Macmillan, 2013), 27.
30 Hutchins B. and Rowe D., 'From Broadcast Rationing to Digital Plenitude: The Changing Dynamics of the Media Sport Content Economy', Television & New Media, 10 (4), (20094): 355-356

The rise of piracy

While some fans are still willing to pay for a subscription to see their favorite sports teams play, and choose quality and simplicity over the illegal free option, many have in fact begun to opt for the latter, which is threatening the industry as a whole. As the price of Pay-TV subscriptions goes up and streaming technology becomes easier to use, online piracy rises. While the development of various technologies has increased incentives for broadcasters to become more innovative through their live streaming techniques, other technologies have provided pirates with a way to intercept and re-transmit legitimate live broadcasts. Today's computers often have cheap and easy to use TV cards, which are able to capture live TV signals from cable, satellite, terrestrial, and Internet broadcasts and with easily obtainable software one can re-transmit these signals in the digital sphere. This has been an evolutionary change in the sports broadcasting industry as pirates can now, in 'virtual real time', distribute the pirated program and in direct competition with authorized broadcasters and online streaming services, undermining these legitimate services, industry revenues and growth as a whole.[31]

Digital sports piracy and the threat to the sports and broadcasting industries

What do we have to lose?

Given that the sale of broadcasting rights continues to represent one of the main sources of revenue for the sports industry, the increasing prevalence of online sports piracy poses a significant threat to the future of the industry. The exact figures for digital sports piracy are hard to come by as are the exact losses for the broadcasting and sports industries but we can get an idea of the grave consequences it may have by examining what is at stake. A Deloitte 2014 report placed the market for global sports rights at

31 Piracy of Digital Content. Rep. OECD, 2009, 62-64

£16 billion in 2014, an increase of 14% from the previous year as demand for top-tier European football and Major League baseball continues to grow and encourages large investments from broadcasters. In the latest bidding competition in 2013, BT won the broadcasting rights for the Champions League and Europa League for £900 million, a huge increase from the current £400 million deal with BSkyB and ITV.[32]

During the 2014 World Cup 20 million viewers illegally streamed the matches, with as many as 500,000 people per match using pirated live streams, illustrating the huge scope of the problem at hand.[33]

Evidently, the rise in cost of sports rights is likely to continue, due to new competition forcing up prices along with the model of Pay-TV, which aims to develop a subscriber base through digital innovation and high quality games. However, as illegal online streaming sites become simpler to navigate and people perceive themselves as no longer being able to pay for subscriptions, live sports broadcasting may begin to move deeper into the illegal online sphere, placing both the broadcasting and sports industry in jeopardy.

Consequences for the broadcasting industry

In the case of Europe, where live sports broadcasting predominately functions under a Pay-TV model, a shift in the audience from the legal to the illegal realm will mean a large decrease in revenues for these organizations with the final result of devaluing sports broadcasting rights.[34] If private broadcasters are not guaranteed the exclusive rights to a particular game or season and their audience and subscriber base declines due to the availability of illegal free options, they will not be willing to pay as much for sports rights in the future. Such a case concerning a decline in audience already took place in the UK in 1996 when BSkyB paid £87 million to broadcast the British rugby league, shifting the rights from the public broadcaster BBC to a Pay-TV channel. Even though BSkyB provided more television coverage of different games, the amount of viewers still declined radically from 2.5 million to 0.036 million in the following years, forcing BSkyB to renegotiate its contract in 1998, which later fell to £45 million.[35] Evidently, a fall in audience and subscriptions for a European Pay-TV sports broadcaster will devalue the cost of sports rights, which will subsequently lead to a loss of revenue for the sports organizations. If individuals continue to turn to unauthorized live streaming of sports events, the very teams and leagues that they support and enjoy watching will suffer from large loses in revenue, affecting the sports industry as a whole. In the UK, the Premier League has already expressed concerns over illegal sports streaming and plans to increase its efforts to battle this underground market after it was discovered that the arrested head of several illegal peer-to-peer sports streaming sites had cost the UK TV industry £10m.[36] The wider effects of digital sports piracy on the sports industry will be discussed in further detail in the next section.

With regards to the US, the rise of illegal live sports streaming would have a different trajectory but the same end result as in Europe. Given that US sports events are broadcast on free-to-air channels, all the actors, including sports organizations, broadcasters, advertisers and sponsors benefit from the greatest share of audiences viewing the channel. High viewership of the events means promotion for the sport itself as well as greater exposure for advertisers and sponsors. However, if viewers turn towards illegal streaming of live sports events, advertisers would no longer want to pay the high advertising fees to the broadcaster, given that the event would

32 *"Premium Sports Rights 'to Surge in Value'" Deloitte. 3 Jan. 2014.*
33 *"20M Found On Illegal Sites During World Cup." Internet and Web Industry News, 25 July 2014.*
34 *Dunne, Margot. "Premier League Fears Web Pirates." BBC News. BBC, 22 Feb. 2009*
35 *Anthony Boardman & Shaun Hargreaves-Heap, "Network Externalities and Government Restriction on Satellite Broadcasting of Key Sporting Events", Journal of Cultural Economics, Springer, vol. 23 (3) (1999), 177*
36 *"20M Found On Illegal Sites During World Cup." Internet and Web Industry News, 25 July 2014.*

have a smaller audience reach than before.[37] Subsequently, if revenue from advertising falls, so does the US broadcasters ability to purchase sports rights for such a high cost, given that less profit is now obtained from the same rights as before. Similarly while sports broadcasting in the US functions on a free-to-air basis, customers still pay a subscription fee for various networks, which include sports in the bulk sum (cable channels in the US are not offered *A la Carte)*.[38] If broadcasters attempt to offset losses in advertising with higher subscription fees for their network, users who would start to deem the subscription service too expensive, would turn to illegal streaming, undermining efforts of both broadcasting industries and sports industries to provide good quality broadcasting and top games.

As the trend of online piracy grows, broadcasting companies and their business models are likely to suffer hefty losses. While pirates do not pay any taxes even though their websites often make revenues from advertising, legal broadcasters and technology enterprises that obtain revenue from invoking their authorized rights, function within a system where they know they can invest and innovate with the chance of receiving a return, under the premise that enforcement exists. Therefore, effective and appropriate enforcement is actually a driver for investment, innovation as well as jobs and taxes, guaranteeing that advertisers, broadcasters and innovators will gain a return on their investment. In 2008, the macroeconomic impact of the sports industry in Europe was projected as $525 billion.[39] Sports pirates undermine this system by coming in direct competition with legitimate broadcasters but without paying taxes and investing back into the industries, ultimately inflicting damages on the survival, innovation and growth of the broadcasting and sports industries.

Consequences for the sports industry

One of the gravest consequences of illegal online streaming is its negative impact on the sports industry. As viewers continue to seek live sports games for free online, this deals a blow to sporting organizations' ability to re-invest and re-distribute into our favorite sports. When copyright holders sell their rights to broadcasters they dedicate a part of this revenue to distribute to the lower level teams to ensure they continue to prosper and improve, as well as invest hefty sums into schools, players and coaches. Online sporting piracy has negatively impacted the revenue right holders receive, as broadcasters lose the incentive to pay large amounts to purchase exclusive broadcasting rights from sporting organizations, knowing they are not in fact exclusive. This loss in revenue from the usually highly profitable sale of rights will negatively impact sports organizations from top to bottom.

Furthermore, a 'culture of acceptance' of digital sports piracy is a dangerous trend as those individuals who currently stream illegal live content may continuously refuse to pay for these services in the future. Such a development would represent a catastrophic blow to the sports industry, which would continue to lose revenue and hence invest money back into the sport.[40]

For UK sports, the greatest burden would fall on the lower league teams, who get significant funds re-distributed to them from broadcasting revenues. A minimum of 10% of revenues from the sale of broadcasting rights gets streamed through to the grass-roots level of the football industry and re-invested into youth programs, education and training, research and development, and sports facilities. If these funds decrease significantly from the use of unauthorized online streaming, the quality of lower level games as well as facilities will decrease.[41]

37 *Dayal, Anish. "Inside Law: Live Sports Telecast and Piracy." Wall Street Journal, 17 July 2014.*
38 *Schrotenboer, Brent. "NFL Takes Aim at $25 Billion, but at What Price?"USA Today, 5 Feb. 2014.*
39 *Evens, Iosifidis, and Smith, The Political Economy, 19*
40 *Update on Digital Piracy of Sporting Events 2011. Rep. Net Result, 2011, 11*
41 *Montel, Julien, and Amnyos E. Waelbroeck-Rocha. The Different Funding Models for Grassroot Sports in the EU. Rep. Eurostrategies, 16 Feb. 2010*

The Premier League is a generous investor in facilities for the overall longer term benefit of the sport, with over £150 million devoted to sporting facilities in every one in fifteen seasons since 1997/1998. Up to 2011/2012, capital investment has included the construction of 29 new club stadia throughout four divisions, the redevelopment of numerous stadia, and deployment of significant funds to player training facilities aimed at maintaining the quality of the games and professional players in the long term.[42]

Given the value of the deals for the 2013-2014 season the Premier League has signed with Sky and BT for £760 million a year, it is understandable that the continued rise of the illegal sports streaming industry will threaten investment for the future. A spokesperson for the Premier League expressed a similar view when asked about the removal of streaming sites, "if you want top quality football, it costs money".[43] Similarly John Perera of the England and Wales Cricket Board (ECB) stated that if individuals continue to go around official channels to view games, "there will be a lack of money in the sport"[44] considering that the organization is non-profit and in charge of running the entire cricket industry, including major teams, junior teams and recreational cricket.

Conclusion

The popularity of sports and new private commercial entrants into the broadcasting industry have created a lucrative market for sports rights which has allowed for significant reinvestment into the sports industry and high quality professional sporting events. Technologic innovations have created a drive on behalf of broadcasters and telecommunications firms to continue to find new and improved ways to provide customers with high-end digital streaming options for live events aiming to eventually become leaders in ground-breaking technologies. At the same time, cheaper technologies have allowed for online sports piracy to prosper and directly compete and undermine legitimate broadcasters. The continued use of unauthorized live sports streams actively threatens the sports industry and the investments sports organizations allocate to improving facilities, training and youth programs, alongside the negative impact of such activity on the innovation of the broadcasting industry to its ability to reinvest into quality live streaming.

Having examined the impact of illegal video streaming on the sports industry, we shall now proceed to examine the technical and cyber security aspects that have transformed video streaming into one of the resilient staples of modern Internet culture.

42 Turn On, Tune In, Turnover Annual Review of Football Finance – Highlights. Rep. Deloitte, June 2013.
43 Chacksfield, Marc. "Illegal Football Streaming given Red Card by the Premier League." TechRadar, 16 Aug. 2012.
44 Dunne, Margot. "Premier League Fears Web Pirates." BBC News. BBC, 22 Feb. 2009

III. VIDEO STREAMING AND CYBER SECURITY

Evolution of technical standards

Video streaming has come a long way since its humble beginnings in the early 1990s, when it was plagued by pragmatic problems - such as insufficient software and hardware capabilities - from achieving mass appeal. Essentially, successfully rendering video requires three main elements: a CPU powerful enough to decode the stream, a data bus wide enough to transmit video data to the video adapter and monitor as well as a sufficient network bandwidth to ensure smooth transfer. In early days, where the best access to networks was through a 56kB or a 28.8kB modem and well before the development of compression algorithms, large scale video streaming was virtually impossible[45].

Multicast and the rise of streaming

The first experiment in live streaming was made possible by **multicast**, a technology that allows data to be streamed from one server to several receivers simultaneously. A single low-bandwidth connection to a special server is all it takes for it to work[46]. The transmission and the duplication of data (simultaneously sending packets to multiple users) is then done by the nodes already existing in the Internet. **Mbone** (or multicast backbone) was the technology used by *Severe Tire Damage* in June 1993, who became the first band ever to perform live online. Developed by Xerox PARC and the Internet Engineering Task Force in 1992, Mbone was in fact a virtual network that sought to use software to compensate for the technical shortfalls of existing hardware. It functioned on top of the Internet and used custom-made software to send packets of data to not just one Internet node, but to 2, 10 or 100. This is generally known as tunneling[47] – Internet routers tunnel the multicast data stream between them over the normal Internet. Unfortunately, multicast was not supported by most ISPs over concerns regarding bandwidth tracking and billing, thus being mostly confined to universities and various research institutions. New solutions needed to be found.

HTTP video streaming

In the 1990s, the vast majority of Internet traffic was HTTP-based (Hypertext Transfer Protocol, over TCP port 80), which governed the communications between browsers and web servers and was used to distribute all the content available on websites to the end-user. Early attempts to provide video distribution over HTTP were unsuccessful as the protocol required video files first to be entirely downloaded on the local machine before playing started, essentially cancelling the advantages brought by on-the-fly streaming. Another big drawback of HTTP video streaming was the quality of service, as the service wasn't designed to service multiple users simultaneously[48]. On the technical side, this was explained by the fact that the bandwidth available to the server was split among all users who were active at the same time, therefore reducing download speeds proportionally to the number of active users connected.

Leveling the playing field: Flash and HTTP video streaming

By the turn of the new millennium though, a combination of elements led to the consumerization of online video streaming: more powerful hardware, wider Internet bandwidths and the development of compression algorithms greatly increased the availability of online content. Unlike previous attempts, several new protocols allowed the data to be played as it was received – the first *true* streaming services.

45 *** "How Internet Video Streaming Works", TechRadar, September 26, 2012
46 Kevin Savetz, Neil Randall and Yves Lepage, "MBONE : Multicasting Tomorrow's Internet (John Wiley&Sons, March 1996)
47 idem
48 see D. Van Deursen, W. Van Lancker, R. Van de Walle, "On Media Delivery Protocols in the Web", IEEE, 19-23 July 2010, pp. 1028-1033

A number of competing video players were developed that sought to brake down the shortcomings associated with HTTP video streaming. Departing from the multicast mode, these streaming protocols used a 'unicast' model – a one-on-one connection between a server and a client, with each client getting a separate stream on request.

The first video player, Real Player developed by RealNetworks, was launched in 1997[49] and gained mass appeal when Windows decided to incorporate the technology (the Real Time Streaming Protocol or **RTSP**) in its highly popular Windows Media Player. RTSP is an application-level streaming protocol that can use both the Universal Datagram Protocol (UDP) and the Transmission Control Protocol (TCP) to transmit and receive packages of data. It was developed by the IETF and published in 1998 as RFC 2326.

At the same time, Apple was rolling out its QuickTime media player, which featured the *Fast Start* technology to describe the **progressive download** playback of encoded digital media content. Macromedia (later bought by Adobe Systems) developed the game changing Flash technology, the first software that used real time raw streaming to deliver video to users. The protocol behind it, the Real Time Messaging Protocol (RTMP, over TCP port 1935) brought a few innovations. Firstly, it was connected to a streaming server tasked only with delivering video content. The servers co-existed with traditional HTTP servers so when a user loaded a web page, it also loaded a video player that greatly enhanced the streaming experience: seeking to random points in the video file became possible as did adaptive streaming, therefore reducing bandwidth usage just to what the user had actually watched. Moreover, the streaming server could easily handle inbound connections from multiple users, improving the overall quality of service[50].

For the better part of the 2000s, RTMP, using the Adobe Flash Player, dominated both the consumer and the business market as it formed the backbone of most streaming sites such as YouTube and Hulu. Unfortunately, despite its modularity and flexibility, Flash proved to be a vulnerable platform for cyber attacks, prompting Wired magazine to place in on its 2012 list of the World's Most Annoying Technologies[51] (we shall address these aspects in a later section). Moreover, RTMP had a series of shortcomings[52]:

- **RTMP packets may be blocked by certain firewalls, though the Adobe Media Server has workarounds if these problems are experienced.**
- **RTMP packets can't leverage standard HTTP caching mechanisms available within the networks of ISPs, corporations, and other organizations, which can improve distribution efficiency and quality of service.**
- **The persistent server to player connection means increased costs, because streaming servers cost money.**
- **The required server may also limit scalability as compared to HTTP-based streaming, since there are many more HTTP servers than RTMP.**

These drawbacks, coupled with the rise of high definition video content, challenged RTMP's reign. As a result, second generation streaming protocols called adaptive bitrate streaming (based almost exclusively on HTTP), such as Microsoft's Smooth Streaming (announced in October 2008 as part of the Silverlight architecture) and Apple's HTTP Live Streaming (HLS, launched in 2009) greatly enhanced earlier HTTP streaming technologies and allowed the distribution of higher quality content. The protocol attempts to combine the advantages of RTSP streaming (quality switching and bandwidth efficiency) with those of progressive download streaming (no special servers needed). Content is fragmented on several servers and relies on the video player to download and then glue them together in order to create a continuous stream. Adobe retaliated in 2010 with the HTTP Dynamic Streaming (HDS) protocol, which tried to blend Flash with HTTP-streaming[53].

49 Alex Zambelli, "A history of media streaming and the future of connected TV", The Guardian, March 1, 2013
50 Doug Mow, "Streaming vs. Progressive Download", Streaming Media, June/July 2007
51 Roberto Baldwin, "12 of the World's Most Annoying Technologies", Wired.com, November 9, 2012
52 Jan Ozer, "What is a Streaming Media Protocol", Streaming Media, August 22, 2012
53 Thomas Stockhammer, "Dynamic Adaptive Streaming over http : Standards and Design Principles", MMSys '11 Proceedings of the second annual ACM conference on

Roughly speaking, the history of video streaming is split between two competing tendencies: **pseudo-streaming** and **real streaming**. The first is characterized by playing while downloading the actual file. Since the entire file is stored in the machine's memory, it has the advantage of enabling quick random seeking and instant replaying of the file. Delivered through the standard HTTP protocol, it has the drawback of being bandwidth intensive[54].

On the other hand, real streaming uses a data buffering viewer, with no file being saved on the local machine's disk. It is highly flexible, allowing for automatic resolution changes (from sHD to uHD for example) to account for variables such as network latency and speed. The obvious drawback is that it cannot perform fast seeking, since the video is not downloaded.

IPTV streaming

Internet Protocol Television is a system developed in the mid 1990s used to deliver digital television to users via the Internet. Using Internet Protocol makes the transmission of TV content possible over a broadband connection. Depending on the vendor, it could be transmitted either by using a unicast or a multicast model, while user datagram protocol (UDP) is the typical protocol used. It establishes a virtual connection between the destination and the source. Its main advantage of this technology is the ability to stream the media directly from the source as it is being broadcast, therefore achieving a higher quality live video stream55. The main problem associated with IPTV is that it operates in a legal grey zone in some jurisdictions. Since there is no globally agreed upon definition of what constitutes copyright infringement, IPTV is one of the main ways used by online video providers to deliver pirated content, especially for live sports events56. Aggregator websites (such as Catchup.com) legally transmit over the Internet content that may be in breach of copyright at the receiving end (see first section).

Peer-to-peer video streaming

Concurrently, a new technology started to make strong advances in the market of online video streaming in the mid 2000s: peer-to-peer technology. In a P2P video streaming architecture, users are both supplies and consumers of data, as the system distributes both content and tasks (download/upload) between users connected to the service. Quality and speed thus depend on the number of users using the service and not on the band

width of the server providing the content, which has made this architecture very cost-effective57. The ease of use has transformed P2P technology into the main vector of illegal video streaming used especially for broadcasting live sports.

Legal vs. illegal video streaming sites

A brief comparison between major video streaming providers shows that the market is currently split between HTTP and Flash-based protocols. Most video content is delivered via plain HTTP progressive download, a pseudo-streaming protocol.

- **YouTube – Uses both a HTTP protocol (Adaptive Bitrate Streaming) and a Flash protocol (Adobe Dynamic Streaming)**
- **Hulu – Uses HTTP Live Streaming (HTTP Live Streaming from Apple)**
- **uStream – Uses a combination of RTMP, HTTP and HLS (HTTP Live Streaming)**
- **Netflix – Uses the OpenConnect architecture and a HTTP-DASH protocol**
- **ESPN – Uses Flash-based RTMP**

Aware of the security vulnerabilities associated with streaming protocols, these major video streaming websites have sought to insulate us-

Multimedia systems, pp.133-144, New York :2011

54 see Lei Guo et al., "Analysis of Multimedia Workloads with Implications for Internet Streaming", WWW '05 Proceedings of the 14th international conference on World Wide Web pp. 519-528, New York :2005

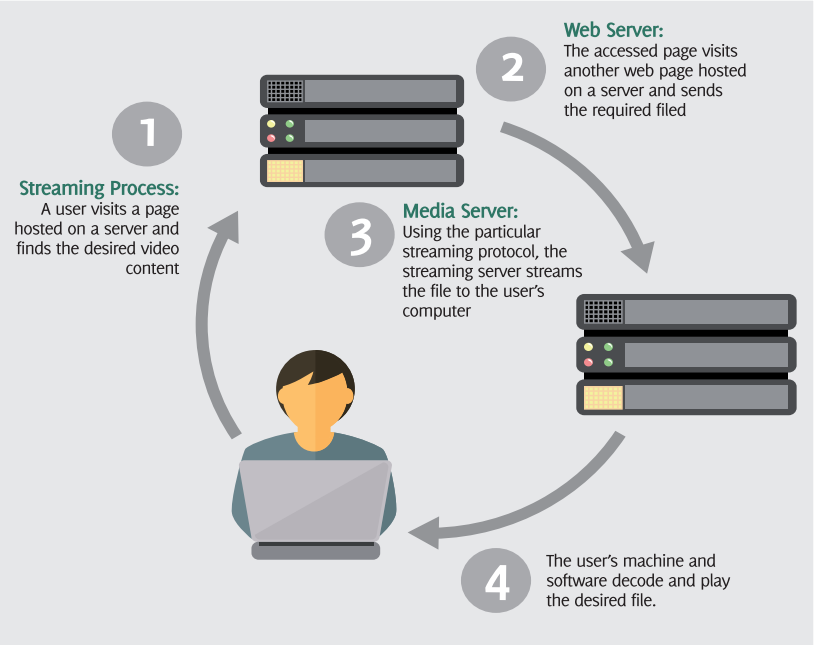
55 Lokesh Mittal, "Internet Protocol Television (IPTV), International Journal of Electronics and Computer Science Engineering, Volume 1, no.4, 2012, p.2221

*56 *** Irdeto Consumer Report, "Attitudes towards Pirated Content", July 10, 2014*

57 see Sabu M. Thampi, "A Review on P2P Video Streaming", arXiv preprint arXiv:1304.1235 , pp. 1-4, 2013

ers as much as possible from threats. YouTube, responsible for 15% of all online traffic thanks to its viral business model reliant on user generated content[58], employs moderation teams charged with monitoring the quality of content uploaded in order to ensure that no copyright infringement takes place and that the videos do not seek to attract users to unsafe websites.

How streaming works



The same thing cannot be said about **illegal video streaming** websites. Websites such as Sopcast, TV Ants and Wiziwig.tv, all based on the **P2P technology**, are the principal sites that enable users to generate and re-transmit streams of unlicensed video content, especially to transmit live sports broadcasts. **Unlike legal streaming services, they offer virtually no security checks, do not employ moderation teams and offer content on a quantity first quality later basis.**

Due to technological advances, such illegal platforms have greatly multiplied in recent times, often with nefarious consequences. Indeed, according to several industry reports, illegal streaming websites are now the **number one propagation mechanism for malicious software as 97% of them contain malware**[59]. Why? Because unbeknownst to users, the rise of illegal video streaming on the highly deregulated and hard to monitor P2P protocol has also given birth to a whole new way for malware distribution. Unlike traditional scamming methods, such as spam email, which require the user to make the conscious decision of clicking on a suspicious-looking link and providing sensitive information, propagating malware through illegal streaming operates using a whole different baiting technique. While the user is **passively immersed** in his video streaming experience, malware programs are actively injected in the background and then controlled by the hacker via the P2P protocol. What's more, illegal video streaming sites are often **riddled with pornographic or otherwise malicious ads**, which raise a variety of concerns for users.

Indeed, cybercriminals are seizing this opportunity to deceive fans of sports events or TV series by broadcasting advertisements promising free streaming of their desired content. As we have presented in a previous section, the World Cup was a boon for hackers everywhere, as it proved to be the perfect ploy to bring large amounts of people to suspicious websites. In fact, **live sports broadcasts are one of the most efficient ways to infect a great number of users**[60]. But how does this baiting mechanism actually work and how has P2P streaming accelerated global rates of infection? To answer that question, we will first have to take a look at malware, its propagation mechanisms and its negative effects on users.

*58 ***, "Global Internet Phenomena Report", Sandvine, 2013*
59 Mike Weatherley, "Search Engines and Piracy", Available at http://www.olswang.com/media/48165108/search_engines_and_piracy_mike_weatherley_mp.pdf
60 Jill Scharr, "With World Cup Malware, the Goal is You", Tomsguide.com, June 12, 2014

The ins and outs of malware

Before we delve deeper in our analysis of the cyber security threats posed by illegal video streaming, we must first identify the object of our present study. As mentioned in the previous section, video streaming has become one of the most potent delivery mechanism for malware and its offshoots. But what exactly is malware?

Roughly speaking, malware (short for malicious software) is defined as "any piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners"[61]. They come in various shapes and act according to different algorithms. The most common types are viruses, worms, Trojan horses, backdoors, keystroke loggers, rootkits and spyware. Each term describes the behavior of that specific malware: while some execute specific tasks (monitoring keystroke activity), others cede control of the infected machine to the person or group of persons responsible for propagating the malware.

Despite their differences, according to the OECD, all malware share several **common characteristics**[62].

- **All types and variations are installed on the victim's machine without the owner's consent. This can be achieved either by exploiting a security vulnerability of the software already installed on that machine or by "baiting" the user to install an infected program, usually a codec or plugin for delivering online video – the so-called 'missing plugin' technique.**
- **Malware is intended to control or monitor the targeted machine and uses it to conduct malicious activities, such as capturing private data or participating in denial of service attacks (we will look into this in the next section). Generally speaking, most malware have a common objective, which is generating revenue for its handlers.**
- **Malware is self-spreading. Depending on the type, malware can automatically infect other systems, either by scanning the network for machines that present similar software vulnerabilities or by sending out spam emails with infected attachments. One OECD study[63] showed that 80% of all web-based malware is hosted on innocent but compromised websites, without the knowledge of their owners.**
- **Malware is easily available. New generations of malware sport shiny graphic user interfaces and are available to download or buy from the Internet for a nominal fee that starts as low as 40$[64]. Reduced costs and promises of high returns on investment have multiplied the number of online threats and have given birth to a new category of hackers, the so-called couch-hackers that can now have the means to launch attacks well beyond their skill level (see section III). In the first three months of 2014, over 15 million new malware samples were created[65].**
- **Power in numbers. The purpose is not to infect just one machine, but to create wide networks of infected machines – called a botnet. Since achieving the computing power required to carry out e-attacks is considerable, malware is used to accomplish such goals. According to Ashley Jelleyman, BT's head of information assurance, "With a big enough botnet and a decent equipment budget, almost any existing level of IT security can be cracked"[66].**

Propagation mechanisms – Is video streaming the perfect bait?

Having looked at the general architecture of malware, it is time to direct our attention to the way malware and ill-intentioned users target the future victim's machine (otherwise known as spreading or propagating malware). Before we proceed, one must keep in mind the fact that as the Internet expanded, permeating ever-new areas of an individual's life, so did malware. Increased machine complexity has brought new ways to spread and bait users into accessing infected content. In this section, we will focus on the relationship between malware propagation and illegal video streaming.

The traditional assumption behind malware propagation was that the user must be actively involved in the process, either by clicking on a link or by

61 **** OECD Report, "Computer Viruses and Other Malicious Software", p.21, 2009*
62 *idem, p.22-23*
63 **** OECD Report, "Computer Viruses and Other Malicious Software", p.25, 2009*
64 *Brian Krebs, " Blackshades' Trojan Users Had It Coming", May 19, 2014, Available at http://krebsonsecurity.com/2014/05/blackshades-trojan-users-had-it-coming/*
65 **** PandaLabs Quarterly Report, January-March 2014*
66 *Peter Gothard, "Buy a big enough botnet and you can crack almost any level of encryption says BT", Computing.co.uk, July 1, 2014.*

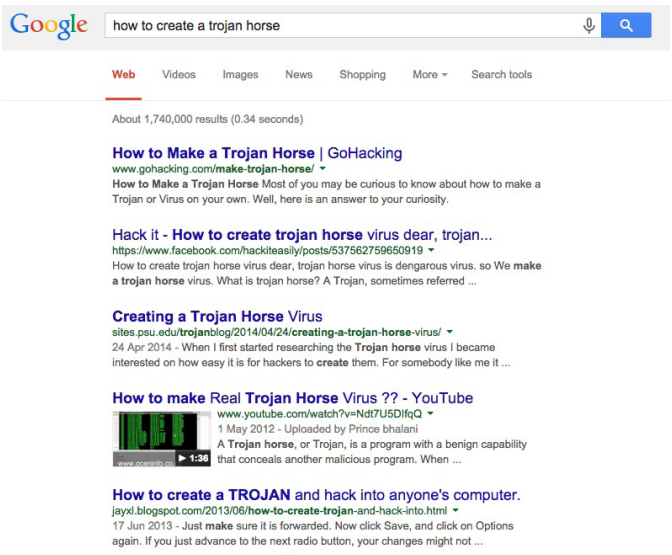
installing a program. **This route** involved sending semi-convincing spam e-mail messages to as many users as possible and then relying on users' lack of knowledge to open it. Over time though these techniques have greatly evolved, especially with the rise of video streaming. Accounting for a great part of all consumer Internet traffic (over 91% according to the OECD[67]), it has become **the number one method to propagate highly dangerous malware on the Internet**. Moreover, it has also made inroads in the corporate world. According to a recent Palo Alto Networks report that analyzed business application usage, even if streaming isn't the most bandwidth consuming activity undertaken in the professional environment, it is nevertheless responsible for the delivery of the most dangerous malware programs available (a category dubbed in the report "malware high in threat delivery"). "The risk of video as bait is more significant than ever before" concluded the report[68].

What must be pointed out clearly though is that simply streaming video content cannot act as a propagation mechanism for malware. Rather, the problem lies either in the software used by the user's machine or the code used by the website hosting the illegal content. Why? Because, as we shall argue in a future section, infecting computers on a wide scale is a very profitable activity.

Drive-by-downloads

Hackers have quickly realized that the best propagation mechanism would be to target security vulnerabilities included in the software already installed by users that enable video streaming. One of the most common targets has been the ubiquitous Flash program, which has grown to represent one of the main ways malware gets attached to a users' machine. According to CVE Details, in the last 10 years Flash has been the target of 338 exploits[69]. Despite innumerable updates, the nature of the algorithm underpinning it makes it an ideal breeding ground for Trojans, key loggers and other spyware. Precisely because of these inherent security vulnerabilities, Apple was one of the first major players on the market to refuse to integrate the software in its iPhone/iPad devices, opting instead for HTTP-based streaming, to the ire of many users.

The infection mechanism is fairly simple and relies exclusively on video streaming; more exactly, streaming of illegal content distributed through an illegal website. Unlike its legal alternatives, such websites integrate "custom" video players that prompt unaware users to install an update for their existing flash video players, a java applet or an ActiveX component. This update, instead of playing the requested video, delivers a Trojan (or any similar malware) to the machine[70]. Depending on the infection type, the program will then work in the background and open various TCP ports, create a Command and Control interface and start communicating with its handler, therefore transforming the target machine into a "bot" or "zombie" (we will touch on this subject in a future section). The vulnerabilities are so easy to exploit that "How-to" guides[71] for wannabe hackers are easily available on any routine Google search.



67 ***OECD Report, "Piracy of Digital Content", 2009, pp. 5-7
68 *** PaloAlto Networks Report, "Application usage and Threat Report", June 2014
69 http://www.cvedetails.com/product/6761/Adobe-Flash-Player.html?vendor_id=53, Accessed on 1st of September 2014

70 *** Microsoft Security Intelligence Report, "Zeroing in on Malware Propagation Methods", Volume 11, pp.17-19, 2011
71 *** "Hack Like a Pro : How to Exploit Adobe Flash with a Corrupted Movie File to Hack Windows 7", March 2014, Available on http://null-byte.wonderhowto.com/how-to/hack-like-pro-exploit-adobe-flash-with-corrupted-movie-file-hack-windows-7-0151305/

Malvertising

Another propagation method used by illegal streaming sites is superimposing over the desired video malicious ads (malvertising) or hidden content that directs the user to an infected website (**iframes**)[72]. Generally speaking, there are two methods used in the propagation of malvertising: one entails criminals placing clean ads on trusted sites for some time before injecting them with a malware code. After a desired number of users is affected, the virus is removed along with the attacker's identity. Another method is by hacking trusted sites and injecting malware into the ads already posted or by adding exploit kits in the source code of the website. Victims are compromised by clicking on infected content, which will then redirect their browsers to another malicious banner that redirects traffic again to an exploit kit. The exploit kit will then "sniff" the infected machine for vulnerabilities before injecting the Trojan[73]. This method saw a resurgence last year, recent examples of hacked websites including The London Stock Exchange, The New York Times, LA Times and Salon.com[74]. According to a 2014 Blue Coat report, the threat of mobile malware from web ads has increased threefold since 2012 and has surpassed pornographic ads as the main avenue of infection[75].

Zero-day vulnerabilities

Research carried out by several major anti-virus companies (including Kaspersky Labs and Norton) shows that hackers have become more and more inventive over the years. Whereas earlier malware targeted outdated or poorly secured machines, today they are able to infect even highly secured systems. Through sophisticated algorithms, hackers use multiple o-day exploits[76] (which are exploits for previously unknown vulnerabilities) to infect systems. Since the exploit is unknown both to the software developer and the anti-virus company, there are no mechanisms to protect the system, leaving it unprotected when faced with malicious software. Many exploits and malware used primarily on illegal streaming websites have gone undetected by both antivirus and antimalware software for long periods of time. Even now, according to the site ZeusTracker, the average detection rate for known Zeus binaries, one of the most common malware programs, is only 38 percent[77]. Moreover, data breaches caused by infected machines with aggressive malware can also go on undetected for months or even years. A study released by Trustwave found that the average targeted attack went more than 210 days without detection[78]. Due to their inherent complexities, finding and exploiting zero-day vulnerabilities points to a concentrated effort, usually with government backing and not to the activities of a motley group of hackers. Stuxnet is one example of such a worm: exploiting four different Windows zero-day vulnerabilities was designed to infect the control servers of industrial plants, oil pipelines, power plants and other critical installations. For users, Flash zero day vulnerabilities are notoriously common. Once exploited, hackers infect the machine with tools meant to siphon off private and personal data[79].

Illegal streaming and propagation of malware

The recent World Cup offered a unique glimpse into the extent to which illegal video streaming was used to infect unsuspecting users, as cybercriminals flocked to use this opportunity to deceive fans online[80]. Using the propagation techniques detailed above – drive-by-downloads, malvertising - users were baited to malicious websites that often resulted in dangerous fraud or malware attacks[81]. Some redirected Internet traffic to other URLs, where users were required to provide credit card information for full access to live streaming, whereas others prompted users to download special software or

72 *Michael Mimoso, "Malvertising Redirecting to Microsoft Silverlight Exploits", ThreatPost.com, May 19, 2014*
73 *idem*
74 *Robert L. Mitchell, "Malvertising Rise Pushes Ad Industry to Action", Computerworld.com, May 29, 2014*
75 **** Blue Coat Mobile Malware Report 2014*
76 **** TrendLabs 1Q Security Roundup, "Zero-Days Hit Users Hard at the Start of the Year", 2013*
77 *https://zeustracker.abuse.ch/*
78 **** Trustwave Global Security Report, 2013*
79 **** Info Security, " New Adobe Flash player zero day vulnerability revealed", October 28, 2010*
80 **** TrendLabs, "Threats Get a Kick Out of 2014 FIFA World Cup Brazil Buzz"May 9, 2014*
81 *Dimitry Bestuzhev, "Adware or Money Loss Instead of Your Favorite World Cup Game", Securelist.com, June 19, 2014*

install "missing plugins". For example, Trend Micro, a security company, detected a file called "World Cup Streaming 2014.exe", a malware backdoor that allowed hackers remote access to the targeted machine. The company also identified a key generator that supposedly allowed people to stream FIFA's official content for free, which actually installed malware. In our research we found that a similar fate suffered users who chose to stream content via P2P from sites such as SopCast, a highly popular albeit shoddy streaming platform – channel 11910 being a case in point.

But why have malware infections become so commonplace? What is the rationale behind mass-scale infections with specific spyware programs?

From single infection to botnets

As mentioned above, one of the traits shared by all malware applications is their capacity to replicate and infect other machines. The reason? Creating ever-wider networks of infected machines to be put under the control of a single handler, called botmaster or botherder. Upon infection, roughly speaking, there are two main scenarios for the targeted machine: theft of personal data (information, money, account information) or the system can become part of a botnet. Such zombie networks that bring together anything between several to a million computers have become a steady source of income for cybercriminals, with several estimates putting **worldwide losses for users at more than $113 billion in 2013 as a result of botnet activities**. Americans have lost an average of $298 per victim, mainly through the stealing of sensitive personal information (credit card fraud, stealing of banking details, hacking of personal accounts), whereas it is estimated that 92% of Russians are affected every year by cyber crime[82]. The reduced operating costs and the ever-diminishing degree of technical knowhow required to put a botnet in place have been the main factors behind their growth in popularity. It is estimated that every year more than 500 million computers are infected, which translates to a whopping rate of **18 new victims every second**[83]. Moreover, according to a report published earlier this year, the global infection rate during the first three months of 2014 was 32.77%, with China in the first place, with a lead of 52.36%[84]. This means that one in three machines worldwide is currently compromised by malware, 73% of them being infected with a Trojan. The report also showed that new malware samples were created at an average rate of 160,000 per day, making detection, disinfection and prevention a daunting task for any company in the cyber security industry.

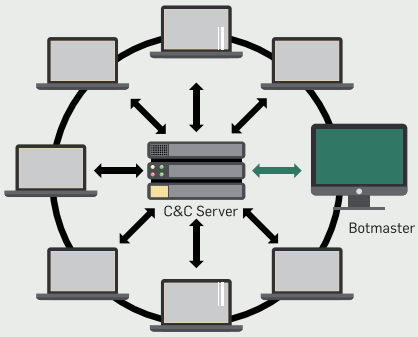
Botnet architecture

Once a network of infected computers is put in place, one of the major challenges is how the botherder issues commands to it without being detected. The first botnets were discovered in 1999, Sub7 and Pretty Park, created respectively by a Trojan and a worm-type malware[85]. Both used rudimentary communications channels, which made them easy to uncover. Since, different architectures, generally called **command and control channels**, have been used by botherders to conceal both their identity and the commands issued, all the while operating under the radar of antivirus solutions. In most cases nowadays, the individual bots no longer interact directly with the botherder, but connect first to a server (the command and control server), which tells the bots what to do. Architectures[86] have greatly evolved over time, from a simple star-shaped topology, where a single C&C server issues commands to all bots, to the decentralized P2P model, where bots communicate with each other and send commands through the network. New architectures include a multi-tier system, separating the botherder from its bots by multiple C&C servers. A botherder simply has to join the network, propagate a command to a single bot and then let the P2P protocol take over the task of carrying the message to the other members. But what can one do once a botnet is in place?

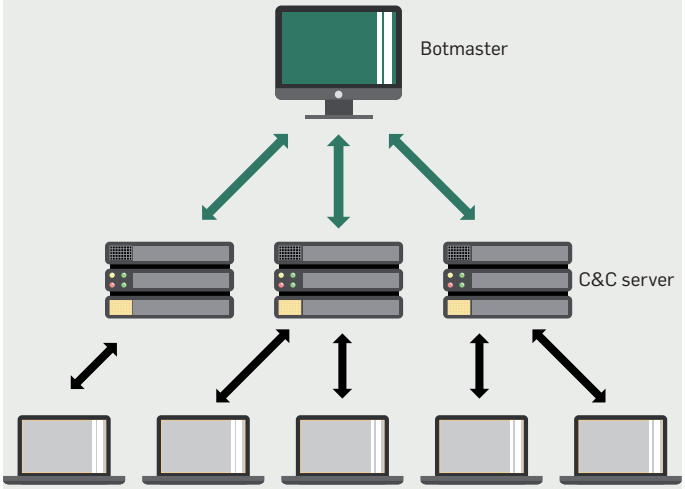
82 *** Norton Cybercrime Report, 2014*

83 *Joseph Demarest, Testimony Before the Senate Judiciary Committee, July 15, 2014.*
84 *** PandaLabs Quarterly Report, January-March 2014*
85 *Tom Brewster, "The Evolution of the Botnet", ItPro .co.uk, October 6, 2010*
86 *Jan Gassen et al, "Current Botnet-Techniques and Countermeasures", Praxis der Informationsverarbeitung und Kommunikation, Volume 35, pp. 3-10c,*

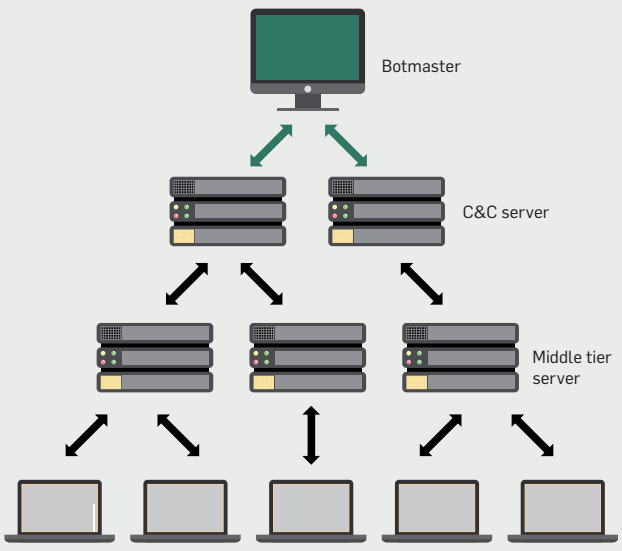
Star-shaped topology



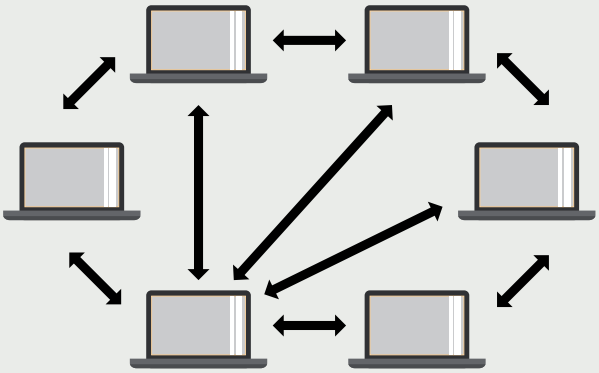
Multiple C&C server



Multi-tier architecture



P2P Architecture



Thanks to their inherent versatility and flexibility, botnets can be put to multiple uses[87]:

- **DDoS – distributing denial of service attacks**
- **Locating and infecting other systems**
- **Sending spam emails**
- **Mining for bitcoin by using computer resources to solve the cryptographic challenges associated with crypto-currencies**
- **Stealing information**
- **Acting as a service that can be bought, sold or rented**
- **Hosting malicious phishing sites**

Botnets operate therefore in a twofold manner: on one hand they seek to infect as many machines as possible (either by sending spam emails without the user's consent or by using the user's machine to scan for other potential vulnerable systems) and on the other hand to generate revenue for the attack by **stealing or selling sensitive user data**. Credit card fraud, siphoning off of bank accounts, identity theft or even compromising a user's social media and email accounts are just several of the most damaging side effects of malware for the consumer. In 2013 a new type of threat achieved prominence, ransomware. Known as CryptoLocker, it has grown by over 700% compared to 2012 and has caused losses to users estimated in June by the FBI at $27 million[88]. Camouflaged as an Adobe Flash update, the malware encrypts the victims' files and then demands pay-

87 *Evan Cooke, Jahanian Farnam, Danny McPherson, «The zombie roundup: Understanding, detecting, and disrupting botnets.» Proceedings of the USENIX SRUTI Workshop. Vol. 39. 2005.*

88 *John Leyden, "CryptLocker-style Ransomware Booms 700 Per Cent This Year", The Register, September 12, 2014*

ment ($100 to $400) to decrypt them. At the time of this writing, there was no known way to crack the encryption algorithm used, which explains the high percentage of victims that have paid the ransom demanded by scammers[89].

DDoS attacks

Probably the most common use for a botnet of any size is using its resources to carry DDoS attacks. These attacks aim to render an organization's website inaccessible, hence the term denial of service by using a network of infected computers (generally ordinary users). It can be deployed using two different techniques: a flooding attack or a logic attack.

- **Flooding is based on brute force and entails sending massive packets of unwanted data to a victim. As a result, network bandwidth is wasted, disk space is filled with unnecessary data and processing power is used up for uselessly processing the packets received. When the attack is mounted in a coordinated and simultaneous manner from different locations and from different servers in order to increase the magnitude of its effects, it is called a distributed denial of service (DDoS).**
- **A logic attack on the other hand is much more precise and uses the target's inherent vulnerabilities against it. For example, exploiting an operating system's bugs, a botnet can crash an entire network by skillfully constructing a fragmented IP datagram.**

Crashing a company's website or network is never the only purpose of a DDoS attack, as it is usually used to gain access to secret or sensitive information. For others, such as Anonymous and LulzSec, DDoS attacks are used to promote a specific agenda or to siphon organizations for politically sensitive e-mails and other materials. The former group made headlines earlier this year when it took down a number of websites owned by World Cup sponsors using DDoS attacks[90], in protest to the funds spent by Brazil on organizing the event.

*89 *** Norton Internet Security Threat Report, 2014, pp. 48-50*
90 Carl Herberger, "Anonymous Delivers DDoS to the 2014 World Cup", Radarware.com, June 13, 2014.

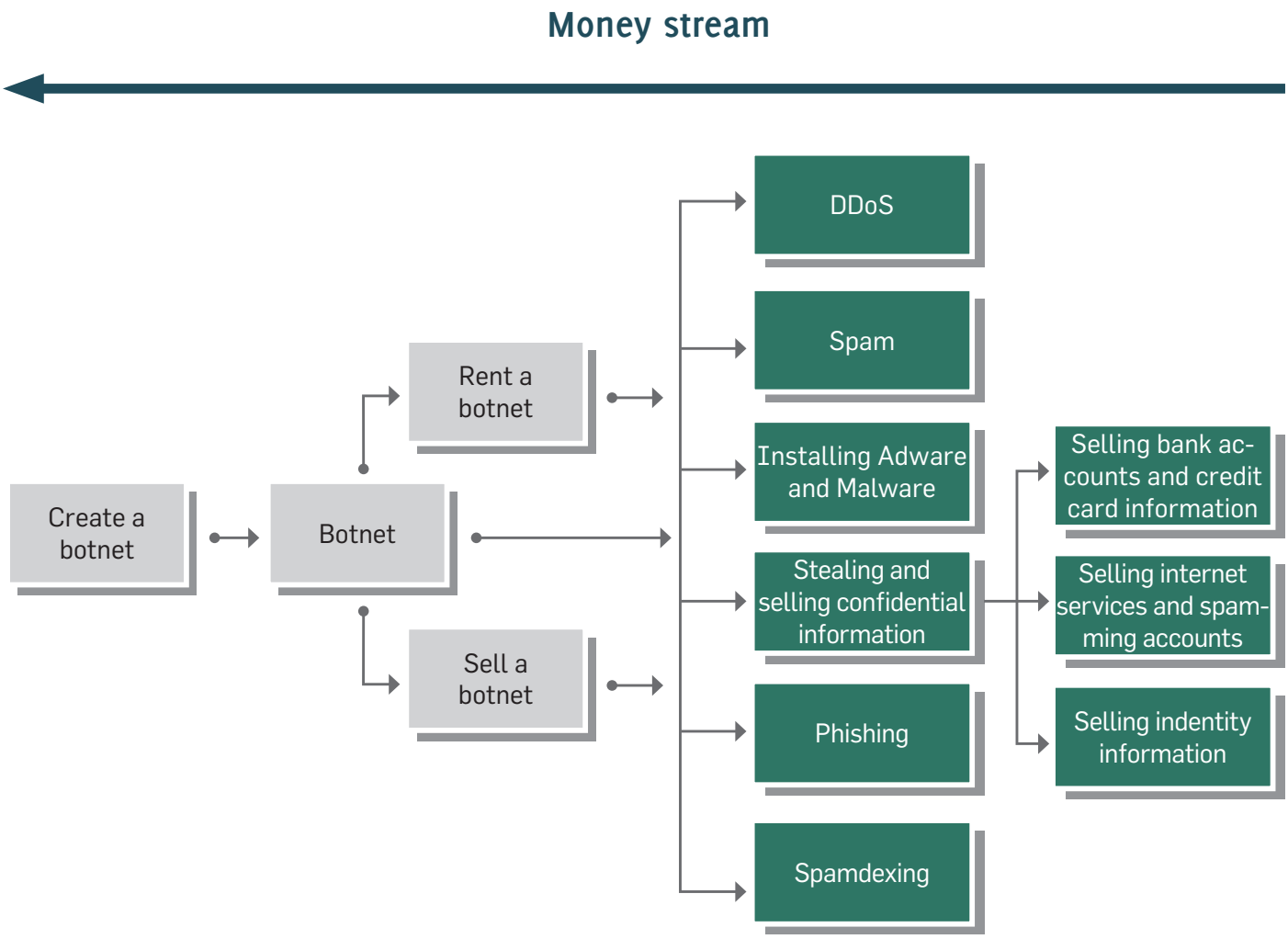
The beginner's guide to assembling a botnet

Due to their versatility, botnets have become essential parts of the ever-expanding online black market. Max Goncharov, a security researcher for Trend Micro released a paper in late 2012[91] suggesting that a complete setup for building and managing a personal botnet can be bought for an initial investment of less than $600, followed by a monthly operating cost of $225. His research was based solely on Google searching using Cyrillic terms and reading freely accessible underground forums. His findings were subsequently replicated by Sean Gallagher of ArsTechnica, proving the fact that the technology is within arms reach for anyone interested in becoming a botherder[92]. But what elements make up a botnet and how can that architecture be integrated in a **video streaming website**?

The first step is finding a **host** for the botnet's Command & Control server. For those lacking the skills to assemble one or to hijack a working server, buying space on a public one is always an option. For example, Hostim VSE ($39/month), a Romanian company, is one of the most used services for botnets thanks to the safeguards employed meant to hide and protect the data they store – *bulletproof hosting*[93]. Once this step is secured, finding a **domain name** to link the bots to the host is imperative. The best option is using a *fast flux* scheme, which hides the server's location by assigning DNS addresses to a rapidly changing set of proxies. With low up times, the system creates hundreds of different communication paths for the bots.

With the C&C infrastructure in place, buying the **malware** meant to create the botnet is the next step. One of the most impervious programs to antivirus

91 Max Goncharov, "Russian Underground 101", Trend Micro Inc Research Paper, Available on http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf
92 Sean Gallagher, "A begginer's Guide to Building Botnets ", ArsTechnica.com, April 12, 2013
93 idem



detection is the Zeus Bot, which can be bought online for as little as $125[94]. Paying a premium will also give access to 24/7 customer support via Skype for any troubleshooting problems a novice user might encounter. The malware will then be coupled with an **injector kit**, an add-on module that will monitor browser activity and inject specific codes on triggering user-defined markers. For example, an injector kit can insert Web code into banking sites that will then try to capture and deliver personal data to the botherder or even make wire transfers. Depending on needs, a botnet can also be equipped with an **exploit tool**[95] meant to bypass a system's defenses by hiding the malware in software such as Flash, Java or the machine's operating system.

Accelerating the propagation rhythm of a botnet can be achieved then in a number of ways, depending on the botherder's own abilities. Creating a simple looking live video-streaming site is probably the quickest and most efficient way of baiting thousands of users. By offering the widest possible selection of sports, botherders turned web-designers seek to maximize the range of users that can be infected or used to generate revenue (clickfraud or riddling their makeshift streaming platform with ads)[96].

In our research undertaken during the World Cup, we have found hundreds of websites created by subscription-paying users legally streaming major sports channels (ESPN or Sky Sports) that also broadcast their signal on improvised platforms. Using several

94 idem
95 idem

96 Suzanne Vranica, "A Crisis in Online Ads : One-Third of Traffic is Bogus", The Wall Street Journal, March 23, 2014

social networks such as reddit (which had an entire channel dedicated to this, now taken down[97]), these temporary websites managed to bypass Google's ranking techniques of search results and secure a steady flow of users. With Viaccess-Orca estimating that illegally streamed football matches attract as many as 20 million people, causing losses to broadcasters and rights holders of over $120 million according to Irdeto, it's easy to understand the appeal for botherders to tap into this pool of potential victims[98].

The bottom line is that an initial investment of $600 can put a normal, untrained user in a botnet's command seat and a fingertip away from causing significant damage to both industries and users.

Impact and industry statistics

The Centre for Strategic and International Studies (CSIS) estimates that the cost of digital crime and intellectual property theft is approximately $445 billion per year[99]. In this context, it is easy to understand why, according to research firm Gartner, organizations spent $67 billion on information security last year [100], with protection from DDoS attacks swallowing a great part of that sum.

The sheer scale and number of DDoS attacks is hard to understate; according to ASERT, at the time of this report 7361 DDoS attacks are conducted every day[101]. What is worrying though is that the threat posed by DDoS has grown year on year. According to Neustar's 2014 report on attacks and their impact, 60% of companies surveyed were DDoS-attacked, up from 35% in 2012. Moreover, attacks are lasting longer (28% having surpassed two days) and are more powerful. The average attack during the first quarter of 2013 was 48.25Gbps, an eightfold increase over the last quarter of 2012; unprecedented attacks of over 250Gbps were also registered. As a result of this rise in DDoS attacks, 40% of companies confessed to having suffered more than $1 million in lost outage a day, as 55% of DDoS targets were also victims of theft, fraud, intellectual property crime, data theft[102]. These combined events led Symantec to declare 2013 the Year of the Mega Breach, as cybercriminals unleashed the most damaging attacks in history[103].

The main culprits behind these massive DDoS attacks were several Trojans, which have risen to prominence in recent years. Zeus Bot[104], responsible for infecting an estimated 4 million computers in the U.S. alone thanks to its state of the art stealth technique, managed to cause losses to consumers and business alike to the tune of some $70 million before being dismantled by the FBI earlier this year. Using the already presented drive-by-download propagation method, it exploited vulnerabilities found in Adobe Reader and Flash to infect machines. Another Trojan that spread by booby-trapping illegal online video streams, Zero.Access, was responsible for the heaviest malware activity registered in 2013. It has infected over 2 million PCs worldwide and is used for bitcoin mining, perpetrating click fraud against online advertisers and generating spam e-mails[105].

Thanks to P2P architecture to hide its C&C server, coupled with a modified UDP communications channel, the Trojan has managed to withstand law enforcement efforts to dismantle it. Although it was "significantly disrupted" in December 2013 by a concerted action of Microsoft and Europol, the botnet is still active[106].

97 *http://www.reddit.com/r/stream_links*
98 *Deborah D. McAdams, "Viaccess-Orca : 20 Million Watched World Cup on Illegal Streams", tvtechnology.com, July 25, 2014*
99 *see "Net Losses: Estimating the Global Cost of Cybercrime", Center for Strategic and International Studies, June 2014, Available on: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf*
100 **** Gartner Special Report on The Future of Global Information Technology, 2013*
101 http://www.arbornetworks.com/asert/, *Accessed on September 2, 2014*
102 **** Neustar Annual DDoS Attacks and Impact Report, 2014*
103 **** Symantec Internet Security Threat Report 2014, Volume 19, April 2014*
104 **** Trojan.Zbot Technical Details, Available on http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99&tabid=2*
105 **** Trojan.Zeroaccess Technical Details, Available on http://www.symantec.com/security_response/writeup.jsp?docid=2011-071314-0410-99&tabid=2*
106 **** "Microsoft, the FBI, Europol and industry partners disrupt the notorious ZeroAccess botnet", Microsoft.com, December 5, 2013*

Conclusion

This worrying trend in the proliferation of cyber crime poses existential problems for Internet security specialists. With threats multiplying every day and with hackers growing increasingly sophisticated, there is a growing need for a more demand-side solution. Even if behavioral analytics would be used on larger scales, the end user will always act as the defining enabling factor for cyber crime. The bottom line is that even if an illegal streaming website does not raise any alarm signals from a user's antivirus or adblocker, it does not mean that the website is safe to use. Once a user's machine is compromised, it becomes part of a malicious network of infected machines (bots) that are used by various groups either for personal profit or for mounting cyber attacks against various targets. It is our view that stymieing the hacking wave that took off in recent years entails mounting awareness campaigns targeted at computer users everywhere, highlighting the threats associated with popular and ethically vague illegal activities such as video streaming.

IV. RECOMMANDATIONS

- Illegal online piracy is a global problem that transposes borders and therefore requires an international response. In many cases, streaming sites are set up in places like Asia, where there is a large broadband capacity, the legal situation is unclear and law enforcement is lax. Countries need to improve international cooperation with regards to these illegal streaming sites and establish a unified system of laws to tackle this problem.
- Awareness and educational campaigns are a key tool to tackling the problem of illegal streaming. Users need to be aware that they are bankrolling a damaging black market economy rather than the sports/TV/film industries that are responsible for producing the content they know and love.
- Sports leagues and broadcasting companies should work together to create the best viewing experience for its fans and customers and ensure that viewers can access sports games on any technology of their choice, whether it be phones, tablets, game consoles and/or laptops. Providing the best quality at a reasonable price will reduce the amount of people who turn to illegal live streaming sites.
- As the Business Insider poll has shown, many users have no particular stance for or against video streaming. Therefore we recommend mounting large-scale awareness campaigns targeted at the end user that will take into account the negative externalities associated with illegal video streaming.
- Since such websites pose major security risks for the user, it would be worth exploring increased cooperation between search engines, major social networks and law enforcement. Taking down individual sites would be too time consuming since streaming websites are quite easy to create and a savvy user can always recreate its service if taken down. Cutting off their access from search engines would effectively sever their connection with potential users.
- Probably the most important recommendation we can make, and one that has continuously been promoted by all actors in the cyber security industry, is that prevention is key. All users should have at least a basic antivirus solution from a major provider. In addition, users should avoid opening attachments from unknown (or unwanted) sources, never download software from untrusted sources and always keep their machine's software up-to-date. As this report has pointed out, illegal streaming is increasingly becoming one of the main avenues of infection, due to its mass appeal and high accessibility of malware programs.
- As this report has shown, users have even more to lose by breaching copyright laws than does the industry; this issue thus becomes a public security issue. With one third of all machines in the world compromised by malware and with ever increasing cyber attacks, it becomes clear that increasing the security of individual users will weaken hackers' resources, both physical (botnets) and financial.
- We also recommend a more coordinated approach on a regulatory level, meant to tackle online copyright abuse. A unified approach in U.S. case law regarding streaming modeled on the patent system could create the healthy legal environment that would balance the needs of consumers with the needs of protecting copyright

Acknowledgments and Credits

This report represents the first ever crowd-sourced independent report on Internet security published by the AISP. Coordinated by Fred Arndt, it is features contributions from Richard Bancroft, James Stamm, Natalie Wells, Matthew Bates, George Wickham, Sofia Hart, Mike Williamson and Juliette Leduc.

Fred Arndt is currently working as a Senior IT security consultant in London, UK, where he has lived for the past decade. After completing an undergraduate degree in English and Government in New York, he converted into the IT sector, working in the US, Taiwan, Germany and now London. In 2014, he started the AISP project, where he counts on the support of several industry experts, friends and partners.

About AISP

The AISP seeks to be the foremost crowd-sourced think tank on Internet Security. We seek to establish an independent platform that will allow industry professionals to exchange ideas, network and propose new solutions for the future.

From policy papers and reports to open discussions on a range of topics, the AISP aims to become a one-stop shop for Internet security professionals everywhere.