CRACKING DOWN ON DIGITAL PIRACY

REPORT

September 2017

CONTENTS

GLOSSARY OF TERMS

CONTENT: a catch-all term to describe the movies, TV shows, song or albums that people might access or download online

DIGITAL PIRACY: illegally making someone else's copyrighted content, such as movies or TV shows, available online

STREAMING: accessing a piece of content without downloading it – for example, listening to music or watching a football match on a website

UPLOAD: putting files online for other people to access

DOWNLOAD: saving files from the internet onto your own computer

SET-TOP BOX: a box that connects to your TV so it can receive cable, satellite or digital channels

ILLICIT STREAMING DEVICE: set-top boxes that have illegal add-ons to access illegal content. Mostly commonly known as Kodi boxes with additional add-ons

CARD-SHARING: a method whereby a person shares part of their set-top box card's access code with other people, allowing them to also watch paid-for channels illegally

VPN: virtual private network, an encrypted connection between someone's computer and the rest of the internet

TORRENT SITES: "torrent" is short for "BitTorrent"; a technology used to distribute files over the internet. While there are many legitimate uses for this, perhaps the most common use is to share pirated movies, music and other copyrighted files

CYBERLOCKERS: online services that allow users to store and share large files. These are often used to generate significant income through illegal subscription services

MALWARE: software which is specifically designed to disrupt, damage, or gain authorised access to a computer system. Pirates can use this to access personal information like financial data

1 INTRODUCTION

Digital piracy is one of the biggest challenges facing Britain's creative industries – such as TV, film, music and publishing – and the wider economy. But the issue is misunderstood by the general public and is surrounded by many myths and misconceptions.

This report seeks to change that by making publicly available information and insights into how digital piracy happens and how the criminals behind it operate.

By its nature as a criminal enterprise, digital piracy is opaque and definitive information often does not exist. This report is based on expert insight from police, law enforcement and creative industry professionals, drawing upon real-life cases, to build a picture of digital piracy today.

The preparation of this report involved consultation with broadcasters and the following organisations:

FACT

City of London Police,
Police Intellectual Property Crime Unit (PIPCU)

Intellectual Property Office

Intellectual Property Office (IPO)

Police Scotland

Entura International

2 SIZING UP THE ISSUE

The vast majority of British people do not watch or download illegally pirated material online, such as movies, TV shows or footage of live sporting events.

The most recent stats show that 75% of Brits who look at content online abide by the law and don't download or stream it illegally – up from 70% in 2013. However, that still leaves 25% who do access material illegally.[1]

This is a problem seriously affecting many of the 3m people who work across nearly 250,000 companies in the UK's creative industries, threatening their jobs and livelihoods and the tax revenues that come with them.

The latest police figures estimated that there were two million computer misuse offences committed in England and Wales in 2016 – more than burglary, robbery, vehicle-related theft, criminal damage or violent offences.[3] Not surprisingly, then, the police and other law enforcement authorities are taking cyber crime, including digital piracy, increasingly seriously.

In digital piracy, the biggest concern and focus for law enforcement and industry relates to the increasing problem of illicit streaming devices – a newer way to access illegal content, which has only existed for a few years. The Intellectual Property Office (IPO) estimated, based on its experience working across the UK on this issue, that over one million of these devices have been sold in the UK in the last two years.

"At a conservative estimate, we believe a million set-top boxes with software added to them to facilitate illegal downloads have been sold in the UK in the last couple of years."

Intellectual Property Office

The Government's commitment to tackling IP crime is exemplified in it forming and funding of the City of London Police, Police Intellectual Property Crime Unit (PIPCU). PIPCU was set up by the City of London Police and the IPO in 2013 to combat the *"organised crime gangs causing significant damage to industries that are producing legitimate, high-quality, physical goods and online and digital content.online and digital content."* [4]

KEY STATS[2]

£87.4bn
creative industries added to the UK economy in 2015, enough to pay for the NHS for nine months

244,800
number of companies in the UK's creative industries sector

2.9m
number of people employed in the creative industries, equivalent to one in every 11 jobs in the UK

£19.8bn
creative industries' exports in 2014

95%
number of creative industries firms that employ fewer than 10 people

1. *Intellectual Property Office, Online Copyright Infringement Tracker, July 2017:* http://www.telegraph.co.uk/technology/2017/07/07/rise-illegal-kodi-streaming-threatens-piracy-crackdown-says/
2. *Creative Industries Council:* http://www.thecreativeindustries.co.uk/resources/infographics
3. *ONS:* https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesbulletintables
4. *PIPCU:* https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/About-PIPCU.aspx

And this is only part of the picture – FACT is at the forefront of the fight against intellectual property crime in the UK too, particularly in digital piracy prosecutions. In fact their success in detecting and targeting those involved in IP crime means that they are responsible for many of the first successful prosecutions of this crime and have multiple cases and investigations ongoing.

That's not to mention the work of law enforcement across the UK, including the Police, Trading Standards and the GAIN which effectively shares intelligence across police forces, within legislative boundaries.

LATEST DEVELOPMENTS

Illegal live streams

In March 2017, the UK High Court of Justice ruled that Internet Service Providers were to block access to illegal live streams of English Premier League football. In the judgment, Mr Justice Arnold clarified that an end user accessing streams via ISDs carry out an act of copying which is not authorised is infringing copyright, meaning those viewing illegal streams are breaking the law.

EU Court of Justice

In April 2017 the EU Court of Justice judgement in the Filmspeler case included confirmation that streaming by end users on ISDs constitutes an infringement of copyright.

10 years in prison

The new Digital Economy Act which comes into effect on 1 October 2017, has extended criminal penalties for online copyright infringement to match those of physical copyright infringement – maximum sentences will increase from two years to 10 years. This could mean longer custodial sentences for the criminals involved in distributing ISDs.

Successful prosecutions

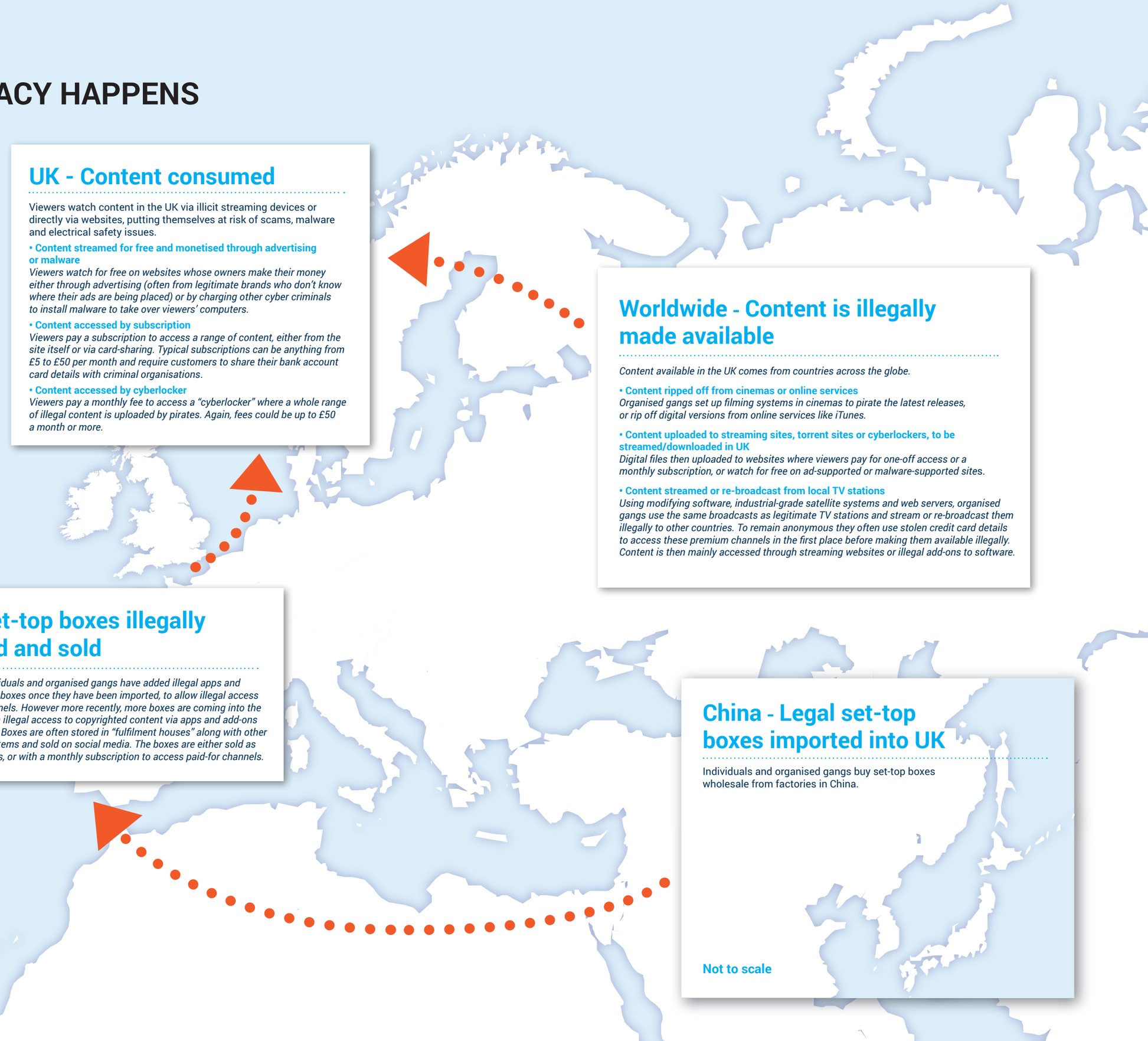
The Premier League and FACT were responsible for the successful prosecutions of Terry O'Reilly and Will O'Leary (2016), which was the first sentencing of a supplier of illicit streaming devices.

3 HOW DIGITAL PIRACY HAPPENS

Few people have a clear understanding of how digital piracy works. Those that consume the end result of the process – by downloading or streaming illegally pirated content – often assume that the material has been made "freely available" by well-intentioned individuals and give little thought to how it has appeared online in the first place.

In fact, digital piracy is often run for profit by criminal gangs and individuals. Both those stealing the content and making it illegally available, and those selling illicit streaming devices, make very large amounts of money from these crimes. Estimates range from tens of thousands to hundreds of millions of pounds of criminal profits every year.

To help explain the criminal process by which digital piracy works, we have outlined the key elements in this section. This is based on the experience and insights of professionals in the police, law enforcement and the creative industries.



UK - Content consumed

Viewers watch content in the UK via illicit streaming devices or directly via websites, putting themselves at risk of scams, malware and electrical safety issues.

• Content streamed for free and monetised through advertising or malware
Viewers watch for free on websites whose owners make their money either through advertising (often from legitimate brands who don't know where their ads are being placed) or by charging other cyber criminals to install malware to take over viewers' computers.

• Content accessed by subscription
Viewers pay a subscription to access a range of content, either from the site itself or via card-sharing. Typical subscriptions can be anything from £5 to £50 per month and require customers to share their bank account card details with criminal organisations.

• Content accessed by cyberlocker
Viewers pay a monthly fee to access a "cyberlocker" where a whole range of illegal content is uploaded by pirates. Again, fees could be up to £50 a month or more.

Worldwide - Content is illegally made available

Content available in the UK comes from countries across the globe.

• Content ripped off from cinemas or online services
Organised gangs set up filming systems in cinemas to pirate the latest releases, or rip off digital versions from online services like iTunes.

• Content uploaded to streaming sites, torrent sites or cyberlockers, to be streamed/downloaded in UK
Digital files then uploaded to websites where viewers pay for one-off access or a monthly subscription, or watch for free on ad-supported or malware-supported sites.

• Content streamed or re-broadcast from local TV stations
Using modifying software, industrial-grade satellite systems and web servers, organised gangs use the same broadcasts as legitimate TV stations and stream or re-broadcast them illegally to other countries. To remain anonymous they often use stolen credit card details to access these premium channels in the first place before making them available illegally. Content is then mainly accessed through streaming websites or illegal add-ons to software.

UK - Set-top boxes illegally adapted and sold

Historically, individuals and organised gangs have added illegal apps and add-ons onto the boxes once they have been imported, to allow illegal access to premium channels. However more recently, more boxes are coming into the UK complete with illegal access to copyrighted content via apps and add-ons already installed. Boxes are often stored in "fulfilment houses" along with other illegal electrical items and sold on social media. The boxes are either sold as one-off purchases, or with a monthly subscription to access paid-for channels.

China - Legal set-top boxes imported into UK

Individuals and organised gangs buy set-top boxes wholesale from factories in China.

Not to scale

The race to release content

Most digital piracy starts with so-called "release groups" – sophisticated online gangs who source the content and get it online as quickly as they can. Their speed, technical capabilities and international reach means they are suspected of also being involved in other forms of cyber crime.

The release groups are organised gangs in competition with each other. They race to get the content out first, so they get the most online traffic and downloads, and therefore the most profit from advertising, malware and subscriptions.

Their activity generally follows a predictable pattern.

1. Cinema Rips

Release groups – have a worldwide network of members dedicated to providing the first recording of high-profile cinema release films. The "cammer" is either motivated by status – being the first to provide a copy of the release – or by financial reward. With the advent of smartphone technologies and miniaturised cameras/spyware (e.g. embedded in spectacles) these operations have become increasing more sophisticated, with content sometimes being uploaded in real time or the digital video stolen from one cinema combined with the audio sourced from another.

2. Web Rips

The release groups will rip off the content from online services like iTunes and make them available for free around the world.

3. Live TV Rips

There has been a significant rise in the number of streams ripped from live TV and video-on-demand. The live streams are usually of major sporting events such as Premier League football games or high-profile boxing matches; recently, hundreds of illegal live streams of the Mayweather vs McGregor fight appeared on social media. Fortunately, major platforms like YouTube and Facebook, supported by the broadcasters, have mechanisms to identify this illegal footage to allow them to shut them down. Recently traffic to many infringing sites has decreased significantly, which means lower profits for the criminals sharing these streams.

4. Blu-Ray Rips

The release groups rip off movies and TV shows on disc formats, although this is in decline and being replaced by live TV rips. Nowadays they tend to focus solely on Blu-Rays rather than standard DVDs, as Blu-Rays offer higher picture quality. These versions are often pirated from review copies so they can be made available as close to the legal release date as possible, when there's maximum publicity about the title and therefore most demand.

Three ways criminal gangs make money from digital piracy

At any one time there are millions of digital piracy sites operating online. While police forces around the world try to shut them down, most gangs operate multiple sites so they can stay online somewhere else.

This approach also maximises their chances of being found online by users searching for content. After all, these are businesses looking for the biggest audience possible.

Almost every website offering pirated content is owned and run for profit – these are criminal enterprises designed to make money. Here are three ways they do that.

1. Advertising

The majority of gangs behind digital piracy make their money from advertising.

A 2013 study[5] in the US of almost 600 "content theft" websites (featuring illegal streams or downloads) found that they earned an estimated $227m in annual advertising revenue. Police forces across Europe and the US are looking into where this money goes.

The 30 largest sites in that study which were supported only by ads made on average $4.4m annually, but even small sites made more than $100,000 a year. This gives them profit margins of between 80-94% – an incredibly lucrative business. (As context compared to legal media businesses, ITV's profit margin is around 20%, while Harry Potter publisher Bloomsbury has a profit margin of 7%.)

These ads are typically banner ads or pop-up windows for casinos, dating sites and download services, often based in Russia or China. But some of them feature ads from legitimate brands, helping them fake an air of respectability.

Many of these ads are placed through "adtech platforms" that automate the process of publishing advertising across the internet, which means legitimate brands often don't know exactly where their ads are going but can give the site an impression of respectability.

5. *Digital Citizens Alliance, "Good Money Gone Bad", February 2014:*
http://media.digitalcitizensactionalliance.org/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/4af7db7f-03e7-49cb-aeb8-ad0671a4e1c7.pdf

2. Subscription

While advertising is the main way the gangs behind digital piracy make their money, some of them also offer subscriptions too. They sometimes try to encourage users to sign-up for a "premium" account, featuring a faster download experience and no advertising, in return for a monthly payment.

Prices vary from site to site, and most will offer a range of packages with different options and costs. But typically these subscriptions will cost anything from £5 up to £50 per month. Subscriptions are also one of the main ways that illicit streaming device wholesalers make their money, charging monthly fees to get access to paid-for channels.

3. Malware

The criminals behind digital piracy often make the content freely available as "bait" to attract large numbers of visitors. They then make money by charging other cyber criminals to put malware on the site, enabling those criminals to hijack the users' computers.

A 2015 study[6] in the US of content theft sites found that one in every three exposed users to malware. In fact, internet users who visited content theft sites were 28 times more likely to get malware from those sites than from legitimate websites or content providers.

The study found that the organised gangs behind content theft websites are making at least $70m a year by charging hackers to put malware on their sites that will then infect visitors' computers.

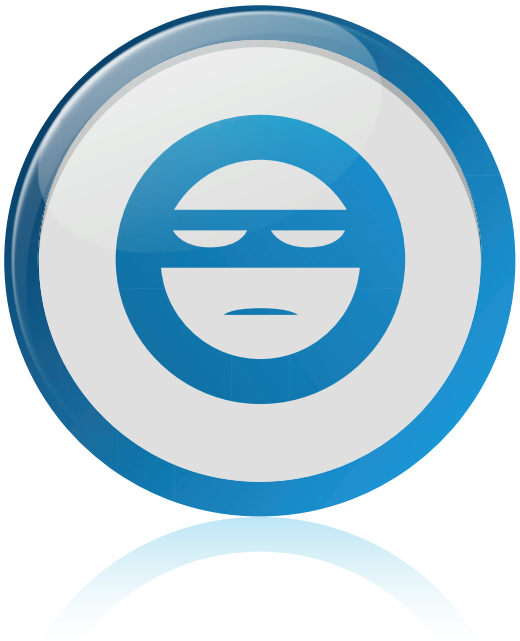
6. Digital Citizens Alliance, "Trouble In Our Digital Midst", June 2017:
http://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Trouble-in-Our%20Digital-Midst%20Report-June-2017.pdf

…And one new way they're trying to make money

Content Ransom

Recently there have been a spate of "content ransom" attempts, with hackers claiming to have stolen movies or TV episodes and demanding ransom payments from companies such as Netflix and Disney.

In April, a hacker by the name of The Dark Overlord claimed to have stolen the new series of Orange is the New Black. He said he would release the episodes on illegal filesharing sites unless Netflix paid him an unspecified ransom. A month later hackers held Disney to ransom, allegedly threatening to leak the new Pirates of the Caribbean movie.



Then in July, HBO experienced a cyberattack in which 1.5 terabytes of data was believed to be stolen, with hackers threatened to leak forthcoming episodes and scripts of Game of Thrones.

The sudden emergence of these content ransom attempts suggests that hackers might be exploring new ways to make money through illegal digital piracy.

The sudden emergence of these content ransom attempts suggests that hackers might be exploring new ways to make money through illegal digital piracy.

4 THE PEOPLE BEHIND DIGITAL PIRACY

Like many aspects of the web, digital piracy is by its nature global and anonymous. It's difficult to track with certainty where a pirated movie or TV show originally came from or who did it.

This is because content is often uploaded through proxy servers and VPNs, which means the organised gangs have hidden their real locations.

The difficulty in identifying specific groups or individuals behind digital piracy, the different laws in other jurisdictions, and the difficulty in co-ordinating action across borders, mean that to date there have been few prosecutions for piracy- and fraud-related offences. What we do know is that it's truly global in nature, with many organisations – be it criminal gangs or anonymous release groups – operating across borders.

Digital piracy is also part of the trade in counterfeit goods which is well recognised as a source of funds for organised criminal groups. According to authorities in the UK and around the world, selling illicit streaming devices is increasingly becoming a part of their broad mix of counterfeiting activity which might also include selling fake clothes, mislabelled alcoholic drinks or counterfeit luxury goods. UK government figures suggest that the annual loss to our economy through all IP crime is £9bn.

Using insights from police forces and other industry bodies, we've identified three key groups of people involved in the digital piracy ecosystem worldwide.

"The Intellectual Property Office's (IPO) partners at the European Observatory on Infringements of Intellectual Property Rights and the Organisation for Economic Co-operation and Development (OECD) estimate that the value of Europe's illegal market is £76bn. UK government figures suggest that the annual loss to our economy through IP crime is £9bn."

Intellectual Property Office, IP Crime and Enforcement Report 2016/17

WHO'S BEHIND DIGITAL PIRACY?

Release groups

Most pirated content starts with so-called "release groups". These are complex, sophisticated and well-organised hacker-style groups who are suspected of being involved in other kinds of cyber crime, like spreading ransomware or hacking people's bank details to sell on the dark web.

Release groups are found worldwide, often with members in different countries.They hide their real locations by using clever technologies like VPNs to cover their tracks.

They are called release groups because they compete with each other to release new movies and TV shows online as quickly as possible. These groups run like businesses, trying to build their brand and develop a reputation for reliable and high-quality content. They often specialise in certain types of content – some focus on releasing TV shows, others on movies, and some even specialise in programmes from certain countries or even specific TV channels.

Site operators

Once the release groups have pirated the content – whether from filming inside a cinema or ripping off files from online services – they then need to get it online. This is where the site operators come in. These groups own and run the streaming sites or cyberlockers where thousands of movies and TV shows are available.

It's not known if the release groups and site operators are always the same people, but we assume that in many cases there is significant overlap between the two. The site operators certainly make the most money out of the process.

They do this either through charging for advertising to be placed on their sites, or by charging cyber criminals to put malware on it that will infect visitors' computers. The more people they attract to their sites, the more they can charge for the advertising or malware.

Site operators who run streaming sites – making live content such as sports events available illegally – often steal innocent people's credit card details first, so they can access hundreds of premium channels under those people's names and cover their own tracks. They then put these streams online for their customers to watch and make money from them.

Site operators typically run several "mirrors" – sites that duplicate each other so that if one is taken down by the authorities, they can still stay online and make money.

Illicit streaming device wholesalers and distributors

A significant number of home-grown British criminals are now involved in this type of crime. Some of them import the boxes wholesale through entirely legal channels, and modify them with illegal software at home. Others work with sophisticated criminal networks across Europe to bring the boxes into the UK. They then sell these boxes online, for example through eBay or Facebook, sometimes managing to sell hundreds or thousands of boxes before being caught.

Some of these criminals have been fined and convicted of offences linked to selling illicit streaming devices. To date most of those people have been operating on their own or in small groups of friends and family, but there have been some cases of offenders with suspected links to much wider international criminal networks.

There have also been some instances of people with a history of class A drug dealing starting to sell illicit streaming devices. In contrast to drugs, streaming devices provide a relatively steady and predictable revenue stream for these criminals – while still being lucrative, often generating hundreds of thousands of pounds a year, they are seen as a lower risk activity with less likelihood of leading to arrest or imprisonment.

However, from October provisions in the Digital Economy Act will come into force extending criminal penalties for online copyright infringement to match those of physical copyright infringement – the maximum sentence will increase from two years to 10 years.

"People seem to think that because parts of the mainstream media don't see this as a big deal, that there's not organised crime behind the selling. Time will reveal the tens of millions of pounds involved in these international networks, and the potentially crippling impact on creation in broadcasting."

Intellectual Property Office

5 CONCLUSION

With criminal enterprises closely linked to piracy, there are several very concerning trends that consumers should be aware of:

Changing digital piracy trends

1. THE TIP OF THE ICEBERG

Digital piracy is a relatively new crime. It has evolved hugely in the last three or four years as technology has developed, and the complexity of these cases means that they often take years to investigate and come to court. That means that the cases we've seen so far are only the tip of the iceberg – we know of many cases that are in the early stages and will come into the public domain in the months and years ahead.

"We have identified a significant criminal business model which we have discussed and shared with key law enforcement partners. I can't go into detail on this, but as investigations take their course, you will see the scale."

Intellectual Property Office

2. KODI ADD-ONS

The availability of illegal add-ons to Kodi software has helped the organised gangs behind digital piracy to reach a wider audience. While Kodi itself is legal, these add-ons are not; they have no parental controls or security standards, and open up users to a range of risks from adult and inappropriate content.

3. SOCIAL MEDIA STREAMING OVERTAKING WEB STREAMING

Previously people looking for illegal streams of sporting events would use search engines to find them on the web. But in the last year or two much of this streaming has started happening through social media platforms like Twitter and Facebook, making it quicker and easier for people to find. This also helps the illegal gangs behind the streaming to reach a bigger audience, attracting more viewers and therefore advertisers, and also putting more users at risk.

4. THE DARK WEB AND BITCOIN BOOM

More and more criminal gangs are using the dark web – hidden from the mainstream internet – to sell illicit information, such as the illegal software used to modify streaming devices or the customer data they've acquired through malware. Increasingly the criminal gangs are also using bitcoin to ensure any funds that come to them, for instance via subscriptions to cyberlockers, are untraceable.

5. SOCIAL MEDIA COMMERCE REPLACING THE PUB OR CAR BOOT SALE

The criminals selling illicit streaming devices are moving their business online. Fewer and fewer are selling these goods through traditional locations like pubs, markets and car boot sales. Instead, they're advertising their wares on social media platforms and e-commerce sites. This helps them attract a potentially much wider audience and try to remain anonymous and avoid capture.

As law enforcement agencies, broadcasters, social media sites, the creative industry and government bodies join forces to clamp down on the criminals behind piracy, we have recently seen many arrests and cases conclude – some of which are detailed below. Many others are in the process of being investigated.

Recent cases

There are many organisations involved in investigating cases relating to digital piracy, with the likes of Trading Standards, IPO, FACT and PIPCU all collaborating to tackle the issue.

For example, since it was started PIPCU alone has worked on 79 complex investigations of the most serious offences connected to digital piracy, and arrested 69 individuals for fraud, copyright, counterfeiting and cyber enabled offences. It has also investigated intellectual property crime worth £33.8 million, and identified over 1,000 websites providing illegal access to films, music, TV, books, games and film.

Also, FACT led a day of action in the north-east and north-west of England, supported by police and Trading Standards, which resulted in multiple arrests in illegal streaming devices.

1. MALCOLM MAYES, HARTLEPOOL

In March 2017 Mayes received a ten-month prison sentence suspended for one year and was ordered to pay £250,000 when he admitted to selling illicit streaming devices that allowed pubs and clubs to screen pay-to-view TV free of charge. He was found to have been selling the boxes to pubs and clubs around the country for around £1000 each, targeting them through adverts in a national magazine which claimed his devices were '100% legal'. Following a test purchase, a suspect device was analysed and found to have been adapted.

2. TERRY O'REILLY & WILL O'LEARY, NOTTINGHAM

This case, in December 2016, was the first sentencing of a supplier of illicit streaming devices. Terry O'Reilly was sentenced to four years in prison and a second supplier who worked with him, O'Leary, pleaded guilty and received a two-year suspended prison sentence. The Premier League brought the prosecution against O'Reilly and O'Leary with support from FACT after the pair were discovered to be selling devices to pubs and consumers which facilitated mass piracy, including the broadcasting of Premier League football on unauthorised foreign channels.

3. PAUL MAHONEY, LONDONDERRY

This was one of the first piracy cases in Northern Ireland led by FACT and PSNI resulted in Mahoney being sentenced to four years. He was found guilty of running an internet piracy scam from his bedroom, offering access to the latest films and television shows, many before general release. He made almost £300,000 through advertising revenue generated from illegal sites, while claiming more than £12,000 in state benefits during that time.

4. SCOTT ALDRIDGE, KENT

In June 2016 Scott Aldridge, a 36-year-old man from Orpington in Kent, pleaded guilty to fraud and money laundering. He had been importing illicit streaming devices wholesale from China, then adding illegal software to them so that users could gain access to paid-for channels for free. He then sold the illicit boxes on eBay and Facebook to local people, allegedly making £19,200 this way.

5.DANIEL DAVID BROWN, SWANSEA

In July 2017 Daniel David Brown, a 28-year-old man from Swansea, was convicted of fraudulent trading for selling illicit streaming devices modified with illegal software, which allowed users to access paid-for channels for free. Brown imported the boxes from China and then illegally modified them at his home. Financial records showed Brown made £371,000 in under two years by doing this.

6. FULFILMENT HOUSE, GLASGOW

In 2016 a fulfilment house in Glasgow was raided in a joint operation by Police Scotland and Glasgow City Council Trading Standards officers. It had been identified as the distribution hub for the sale of illicit streaming devices. During the search officers uncovered illicit streaming devices along with various other counterfeit electrical goods including iPhones and chargers. Enquiries revealed that in excess of seven tonnes of illicit streaming devices had been distributed from this facility. The fulfilment house was being run by Chinese nationals and items were being sold by various sellers in the UK on eBay.

7. GAVIN GRAY, BELLSHILL

In March 2017 Gavin Gray, a 25-year-old man from Bellshill, North Lanarkshire, pleaded guilty to four charges of fraud and copyright offences. He was running a card-sharing operation which he advertised on dedicated card-sharing websites and forums, supplying illegal access to premium channels to customers across Scotland. When police searched his home they found £44,500 hidden in a safe in his loft, and later seized another £80,000 from his bank account. Police Scotland described Gray as "the lynchpin in large-scale, organised illegal activity known in the industry as 'card sharing' with clients across the UK and internationally".

8. ILLEGAL INTERNATIONAL TV STREAMING HUB, CHORLEY

In August 2016 a joint PIPCU and FACT investigation resulted in an address in Chorley, Lancashire being raided and three men were arrested on suspicion of conspiracy to defraud and money laundering offences. While the investigation is still ongoing, police recovered approximately 30 servers and illicit streaming devices which are believed to have been modified with illegal software to enable them to access hundreds of paid-for subscription-only channels. Officers also identified 15 satellites.

9. FIRST RELEASE GROUP SENTENCING, WOLVERHAMPTON

In 2015 five members of an underground piracy group were jailed for more than 17 years, making them the first release group to be successfully prosecuted. The five men, who went under several online aliases including 'memory100', 'Cheese', 'Reidy', 'Cooperman' and 'Kareemzos', often paid for illegalrecording of films in cinemas, known as 'cams', and improved the quality through editing and encoding before releasing online. Over a number of years the groups illegally released online more than 2,500 films including Argo, the Avengers and Skyfall. The outreach of their criminality was vast, and the prosecution followed an investigation led by FACT.

10. JHON ROSERO, LONDON

In December 2016 Jhon Rosero, a 40-year-old man from London (SE14), pleaded guilty to an offence under the Serious Crime Act 2007, namely encouraging or assisting in the commission of an offence contrary to Section 11 of the Fraud Act 2006, by dishonestly obtaining services from Sky without their authority. He was fined £516 at City of London Magistrates Court for setting up an online marketplace seller account to sell devices that would enable the user to get content without paying for it.

"It's obviously very tempting for people to think they are getting a bargain but it's important to remember that there are organised criminals behind these fraudulent schemes, often supporting and funding other more serious crime, such as human trafficking and drugs, so people need to be aware of that. Purchasing a 'so called bargain' may lead to a visit from the police at your door so think twice before saying yes."

Police Scotland

"We have seen an increasing number of unofficial apps and add-ons emerging that allow illegal access to copyrighted content such as live sport, films and premium pay-to view TV via mobile phones, tablets and TV set-top boxes.

Consumers need to be aware that streaming paid content for free is absolutely illegal. Whilst our priority remains to crackdown on the individuals behind this criminality, end users may find themselves getting swept up in one of our operations and becoming part of the whole criminal investigation."

FACT

For more information on this issue, please visit the FACT website:
https://www.fact-uk.org.uk/consumer-advice/digital-piracy-and-ip-crime/

CRACKING DOWN ON DIGITAL PIRACY

REPORT

September 2017