NORDIC CONTENT PROTECTION

Annual Report 2020

Nordic Content Protection

NORDIC
CONTENT
PROTECTION

Nordic Content Protection
www.ncprotection.com
January 2020

Introduction

Welcome to the fifth annual report by Nordic Content Protection (NCP). These reports are meant to analyze and describe the current threat landscape faced by the TV industry. It is our ambition to shed light on the current state of affairs by sharing relevant knowledge, so that legitimate businesses, law enforcement and other relevant actors are better able to understand the current threats and thereby better able to mitigate them.

It is a well-known fact that TV piracy has existed nearly as long as pay-TV. For decades the TV industry has faced and fought the TV pirates and their negative impact. This ongoing struggle is mainly a technological one, where both parties are racing to identify, employ and monetize new technologies to support, develop and protect their businesses.

Illegal IPTV is the latest in a line of examples of this technological arms race. It is an example of how TV pirates have been able to swiftly adopt the technological advances of better and faster Internet to very effectively create and maintain several illegal business models, with a somewhat persistent ecosystem of sellers and resellers and a product that is attractive for consumers.

Meanwhile, for the established TV industry to implement new technologies, it has to financially invest significantly to develop well-tested quality solutions with novel features. These solutions must also protect customer privacy and affiliate rights holders alike. This is not only challenging, but it also carries several business-critical risks if for example a new streaming feature is easily copied by TV pirates or if a new security solution is compromised.

Illegal IPTV continues to be the overall major threat to the TV industry. It is no longer a new phenomenon, but rather a well-established and very visible business model that is heavily promoted on social media and that generates enormous illegal revenue. Illegal IPTV will be the full focus of this report.

Welcome.

About this report

Throughout the following report a number of statistics will be presented. As these are based on data collected by NCP related to actual bad actors, we have to leave out certain metrics to ensure privacy and to avoid disclosing certain sensitive details for NCP to be able to remain an effective IP rights enforcer and a primary intelligence data collector.

NCP members have unrestricted access to all NCP statistics and relevant partners are welcome to request further details.

Executive summary

NCP processes more data than ever before. It is necessary if we want to remain able to make wise decisions when prioritizing the use of our resources. It is the only way to effectively enforce the intellectual property rights of our members. Only through analysis of intelligence data are we able to observe and understand the current threats for then to be able to work against them.

Illegal IPTV continues to grow. The NCP IPTV blacklist of websites selling illegal IPTV has seen an increase of 358% since 2016. And there are no signs that it will be slowing down. The continuing developments of the Internet infrastructure (better and faster) and the relatively low costs of website hosting and server rental all support the illegal IPTV business models.

Running a business selling illegal IPTV is lucrative due to low expenses and plenty of customers, who find the product attractive. For the provider or reseller, an additional benefit is that offering illegal IPTV is a low-risk crime. All enforcement initiatives must come from the TV industry, as no authorities focus on this crime on its own behalf.

Nearly 75% of the websites included in the NCP IPTV blacklist offer Nordic content. This is a strong indicator that there is a specific demand for content from the Nordics.

The use of social media to promote and sell illegal IPTV is also increasing. Facebook has been especially popular for illegal IPTV providers in their efforts to reach as many potential customers as possible. NCP is currently monitoring relevant Facebook pages with approximately 1.3 million followers combined.

A recent European study concluded that across the 28 EU member states, more than 13.7 million individuals access illegal IPTV. This results in an estimated annual illegal revenue of €941.7 million, of which €85.7 million is generated across Denmark, Finland and Sweden. Adding estimations for Norway, the total illegal revenue for the Nordics reaches €102 million, which compared to NCP estimates from 2017 represents a 31% increase in illegal revenue in the Nordics in two years.

Effective enforcement against this problem can only be achieved through cooperation and support between the TV industry and law enforcement. Illegal IPTV is a borderless crime, which traditionally is challenging for authorities. Therefore it is vital that intelligent prioritizations of targets are always a focus, to ensure our actions have the highest effect possible.

About Nordic Content Protection

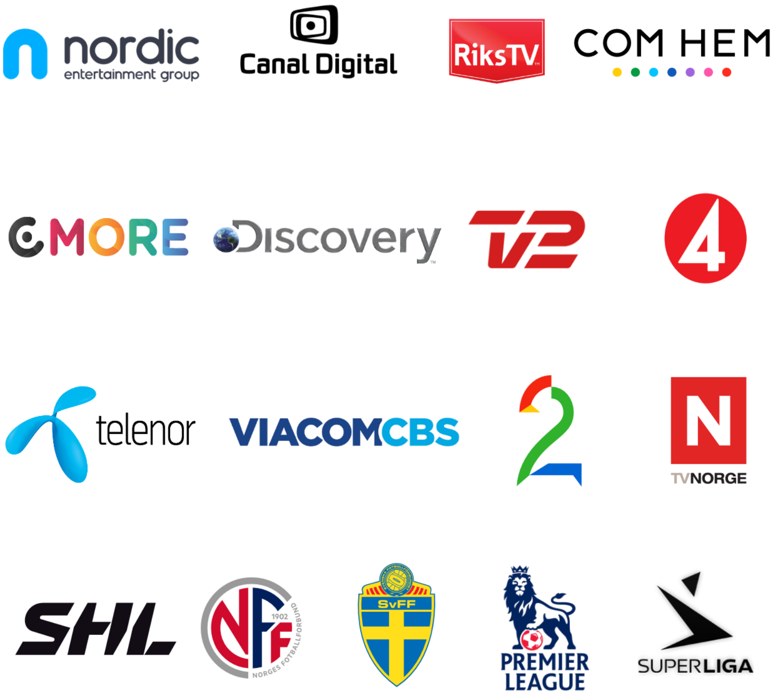
NCP is a not-for-profit membership association dedicated exclusively to intellectual property rights enforcement for the television industry. With more than 20 years of experience NCP works to prevent illegal access to television.

Our team consists of technicians combined with experienced high-tech crime investigators from Nordic and international police forces. Our team composition allows us to remain very specialized and able to investigate and enforce against an ever-changing threat landscape. We work closely with our members and carry out numerous enforcement actions ranging from content take-down to large scale multinational investigations against international organized crime groups.

NCP shares information and data with existing partners (both private and public entities) as we are convinced that this is the only way to effectively enforce IP rights.

To learn more about our work and results, visit our website at www.ncprotection.com or find us on LinkedIn.

NCP members



Illegal IPTV - ecosystem

Illegal IPTV is characterized by being IPTV (TV over the Internet) that infringes existing copyrights. As opposed to the many legal “IPTV” (streaming) offerings from large international companies such as Netflix and HBO as well as more geographically focused, such as TV 2 Play (DK) and Viaplay (Nordic). Illegal IPTV is available on all popular platforms - just as their legal counterparts. Furthermore, as the illegal IPTV services are promoted and sold in a similar fashion as the legal offerings, which can make it difficult for normal consumers to identify whether the service they are considering is legal or illegal.

The most obvious illegal IPTV business model is the direct sale of subscriptions to customers. A subscription will usually be of 1, 3, 6 or 12 months length and the purchase and payments are almost exclusively carried out online via dedicated websites or social media platforms (Facebook and Skype as popular examples). Subscriptions often contain thousands of live TV channels as well as thousands of TV shows/series and movies (video on demand - VOD). Not rarely do subscriptions hold more than 20.000 channels and titles combined.

Main actors

There are two main providers of illegal IPTV to customers. These are, as described in last year’s NCP report, “large scale providers” (LSPs) and “resellers”. Both of them actively facilitate sales to individual customers and as a prerequisite are positioned to communicate directly with and give support to customers. They also have access to payment systems and the ability to generate/give access to purchased subscriptions (deliver the service).

> LSPs are responsible for transcoding potentially encrypted legal TV signals into digital streams, which are included in illegal IPTV subscriptions. Delivery to customers is then provided via an extensive streaming infrastructure, often making use of advanced content delivery systems and relying on several different Internet intermediaries such as hosting- and payment system providers.

In addition to selling illegal IPTV subscriptions to customers, LSPs frequently trade their streams with other LSPs, allowing them to expand their included content by aggregating streams transcoded by others. LSPs usually also offer reseller plans. Such plans enable individuals to resell illegal IPTV subscriptions by using the already established streaming infrastructure.

NCP estimates that only a relatively small number of LSPs exist, but they are, nonetheless, entirely responsible for the illegal transcoding of encrypted TV signals and the subsequent illegal streaming.

Resellers depend on LSPs to provide the streams of TV channels in digital form over the Internet. They generally operate as either a basic reseller or as a so-called restreamer.

- The basic reseller uses the streaming infrastructure of the LSPs and pays the LSP a set price per active subscription (customer) sold. They usually resell for a single LSP and use both dedicated websites and social media as sales platforms. NCP is continuously monitoring more than 1400 active basic resellers

- The restreamer provides his own streaming infrastructure and pays the LSP a set price for the streams (channels and VODs) he wants. This enables the restreamer to aggregate streams from several LSPs, but he must additionally carry the cost of the streaming infrastructure

As an LSP, having either basic resellers or restreamers or a combination is very attractive. It is both lucrative and convenient as it generates increased profit (new customers) without the LSP having to devote resources to sales and customer support. A further added benefit is risk mitigation, which is achieved when LSPs no longer have to promote and sell their illegal services directly to customers and therefore can assume a less exposed role.

The LSP business model is double-sided as it allows for direct sales to customers (B2C) as well as sales to other LSPs and resellers (B2B). The reseller business model is mainly a B2C model, as they primarily sell subscriptions directly to customers.

Additional actors

In addition to LSPs and resellers, it is possible to identify more than 20 different actors, that in combination make up the entire illegal IPTV ecosystem[1]. Some of these will be employed by either LSPs or resellers and some will offer their expertise or services as third parties. An actor will often cover several roles and might work on both the front -and backend of a specific illegal service.

Examples of other actors involved in enabling illegal IPTV as a business could be software developers, who might code a website with webshop functionalities or an online IPTV panel, where LSPs can administer streams, customers and perhaps even resellers.

Another example could be a network administrator, responsible for setting up and maintaining the streaming infrastructure and balancing streaming loads during peak hours.

Illegal IPTV - websites

Since the rapid proliferation of illegal IPTV in 2015 and the following years, it has been a priority for NCP to closely monitor developments to be able to know and understand the threat landscape. To do this we have monitored a range of different data points over time, of which websites used as selling points for illegal IPTV are among the most important.

NCP IPTV blacklist

These dedicated websites are created as the main selling point of providers of illegal IPTV. The services are promoted on different popular platforms such as social media and online marketplaces. Part of the promotions is leading customers to the websites, which are built to mimic traditional webshops with features expected by the normal user today. Having a website of modern design that is user-friendly is one way the providers of illegal IPTV achieve credibility. Another is to be readily available to potential customers, often done via live chat support plugin on the website.

The NCP IPTV blacklist consists of websites selling illegal IPTV - both subscriptions only and subscription bundled with an illicit streaming device (ISD). The population of the list takes place using automation and algorithmic scoring and a special prioritization of detection of websites with a Nordic impact (Nordic content or language) is made.

The blacklist is curated on a continuous basis through manual review, so it is constantly up to date and represents the current state of the specific threat landscape. Several data points

[1] Illegal IPTV in the European Union, EUIPO, Appendix III.

related to the websites are collected simultaneously, making the NCP IPTV blacklist a main point of intelligence for NCP.

While many illegal IPTV websites are short-lived and thus removed from the NCP IPTV blacklist, the number of detected and verified websites have steadily increased since the launch of the blacklist in 2016.

Using 2016 as a baseline number, we have seen an increase of 358% for 2019. The rising numbers of websites in the NCP IPTV blacklist are illustrated below in Fig. 1.

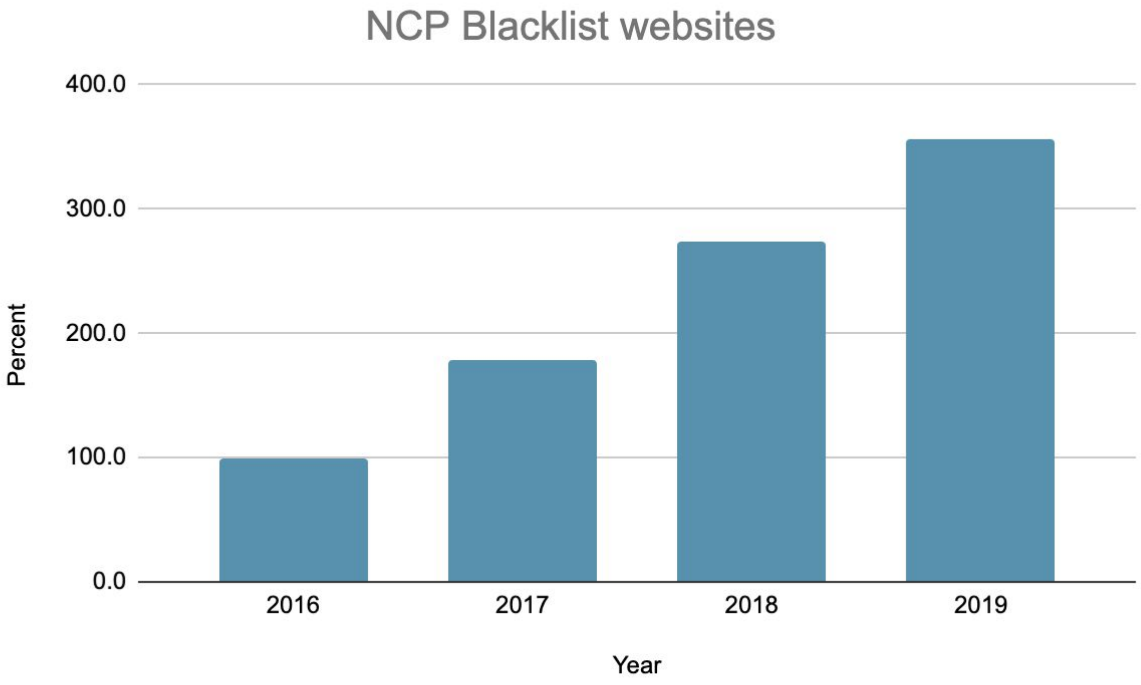


Fig. 1

The highest number of websites was added in 2017, but the numbers for 2018 and 2019 also remain high. This is a clear indication that despite significant enforcement efforts and numerous new legal TV and streaming offerings (including legal IPTV) the illegal IPTV business model, including the use of dedicated websites remains attractive.

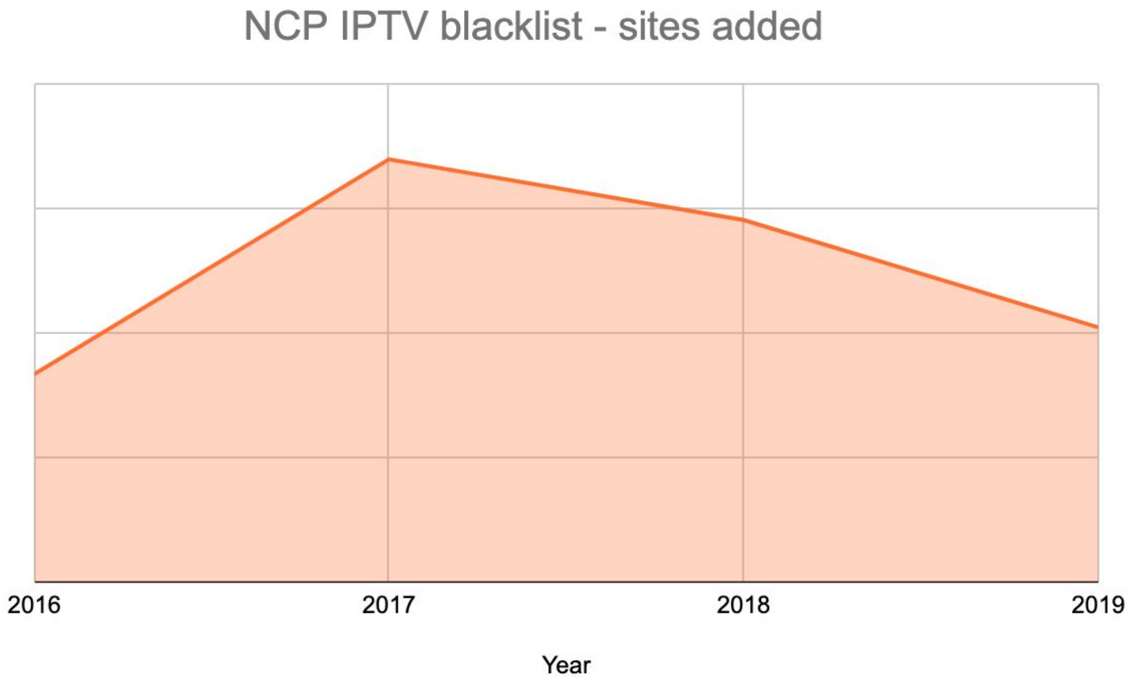


Fig. 2

Collecting relevant meta -and content data from websites offering illegal IPTV is imperative, as it allows for subsequent analysis and target prioritization. And, as mentioned above, these websites are regularly short-lived, so to be able to collect the data, it is crucial to detect them as soon as possible when they become available online.

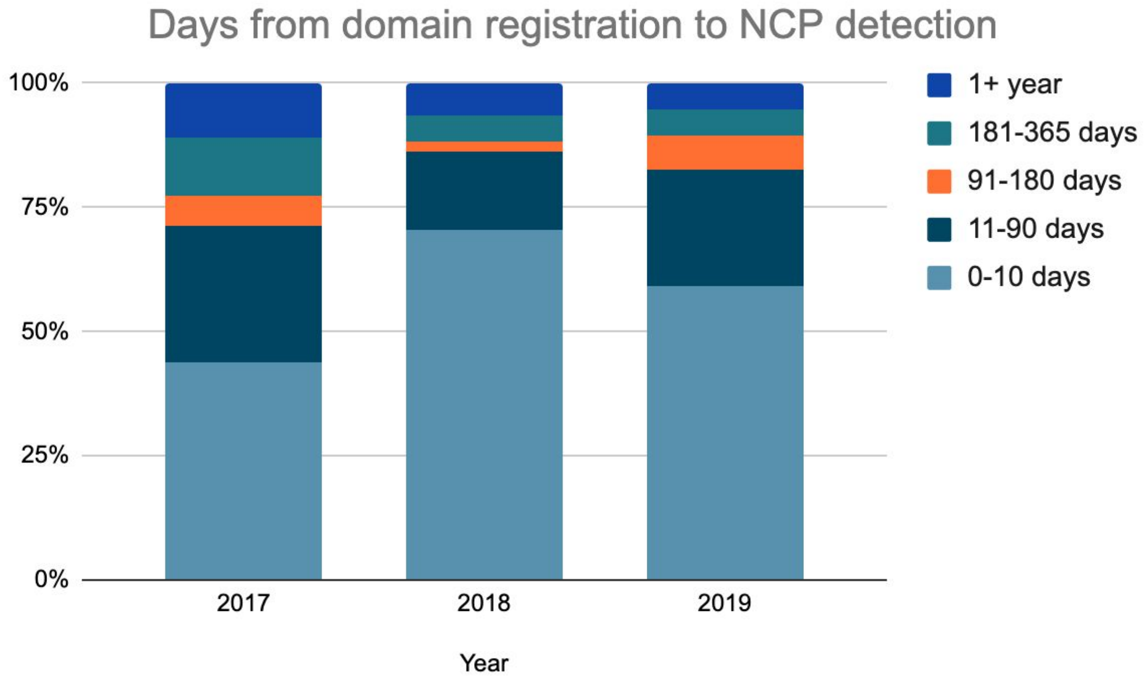


Fig. 3

As a general rule, there is some latency from the time of domain name registration to the launch of an active website online. The reasons for this are usually time spent on configuration, testing and final deployment. However, in the end, it comes down to how and when the domain owner chooses to use the domain name. In fig 3., we are able to see that in 2019 we detected 60% of the websites added to the NCP IPTV blacklist within 10 days from the domain being registered. 23% was detected within 11-90 days of being registered and only around 5% takes more than a year to detect (likely because they simply are not launched sooner).

From fig. 3 it is clear that illegal IPTV providers, in general, are very quick to set up and launch their websites. This includes getting listed as Google search hits and thus becoming very visible to potential customers.

> As website detection and data collection is mostly an automated procedure, it requires constant adjustments and continuous development of the tools used. NCP mainly develops its own set of tools, as experience shows, that such tools, while perhaps narrower in scope are much more effective and can easily be modified to a changing threat landscape. An example of this is collecting data from social media platforms and analysing their association with websites already included in the NCP IPTV Blacklist.

Nordic impact

As protection and enforcement of NCP member's rights is our main objective, the NCP IPTV blacklist is grouped into relevant verified categories. This allows us to have a clear and up-to-date picture of the immediate threat landscape facing NCP members.

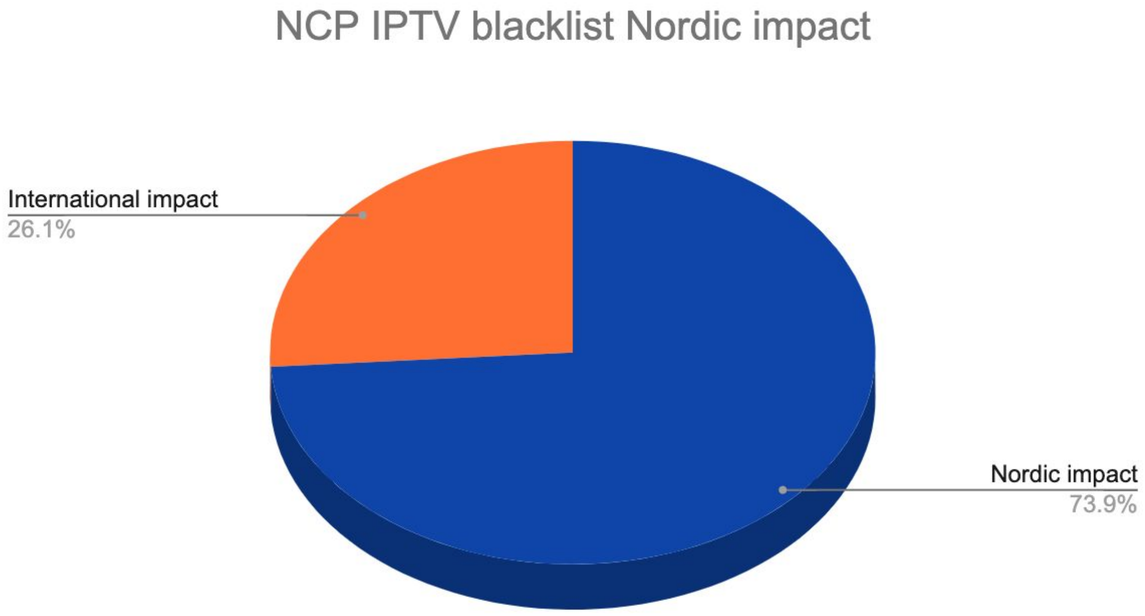


Fig. 4

As seen in fig. 4, nearly 75% of the NCP IPTV blacklist have been verified to have an impact on Nordic right holders, including NCP members.

Such a large Nordic impact underlines the current threat to Nordic right holders and it appears to be the combined result of existing trends in the current illegal IPTV ecosystem and the way NCP identifies relevant illegal IPTV websites. Specifically:

- Nordic content is in high demand
- Many illegal IPTV providers include content from countries spanning the entire globe, including the Nordics
- The NCP detection algorithm is configured to primarily find websites with Nordic impact

Illicit streaming devices vs. subscriptions only

With illegal IPTV becoming the dominant threat over card sharing during recent years, a shift regarding the sale of set-top boxes (illicit streaming devices - IDS) followed.

Illegal IPTV is offered on all popular devices such as smartphones, tablets, computers and smart TVs and a clear result of this is that IDSs for TVs are in less demand. This is also represented in the NCP IPTV blacklist:

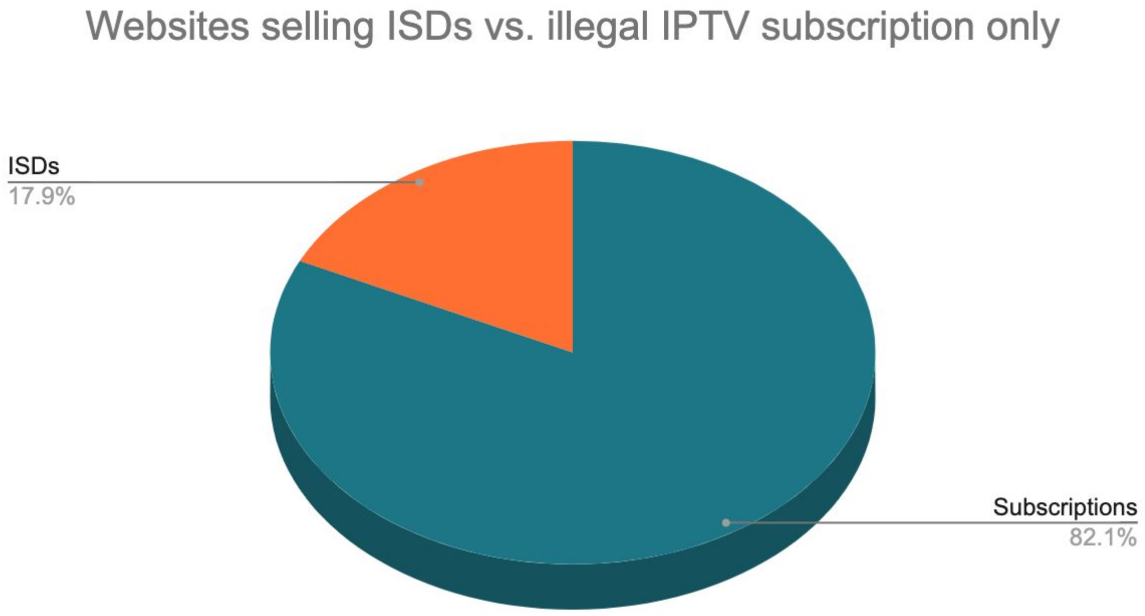


Fig. 5

Comparing the fact that less than 20% of the NCP IPTV blacklist websites offer sale of ISDs to the fact that when card sharing was the major threat to the legal TV industry all customers needed a set-top box it is clear that this is an advantage for illegal IPTV providers.

Being able to sell illegal IPTV without the need to include a physical device is a contributing factor to the proliferation of the illegal IPTV ecosystem, as it means lower costs for the criminals and less risk of detection during the import and delivery process of the ISDs

Payments

Many of the NCP IPTV blacklist websites advertise their payment methods on the website. Usually, this information is put either in the front page footer or in a specific section on the site. Other websites do not declare their payment options until a customer finalizes a purchase. The payment details are then either sent via e-mail or shown during the checkout process.

NCP combines automated retrieval with manual checks to identify payment options. As a result, we are able to conclude three main payment options are mainly being utilized:

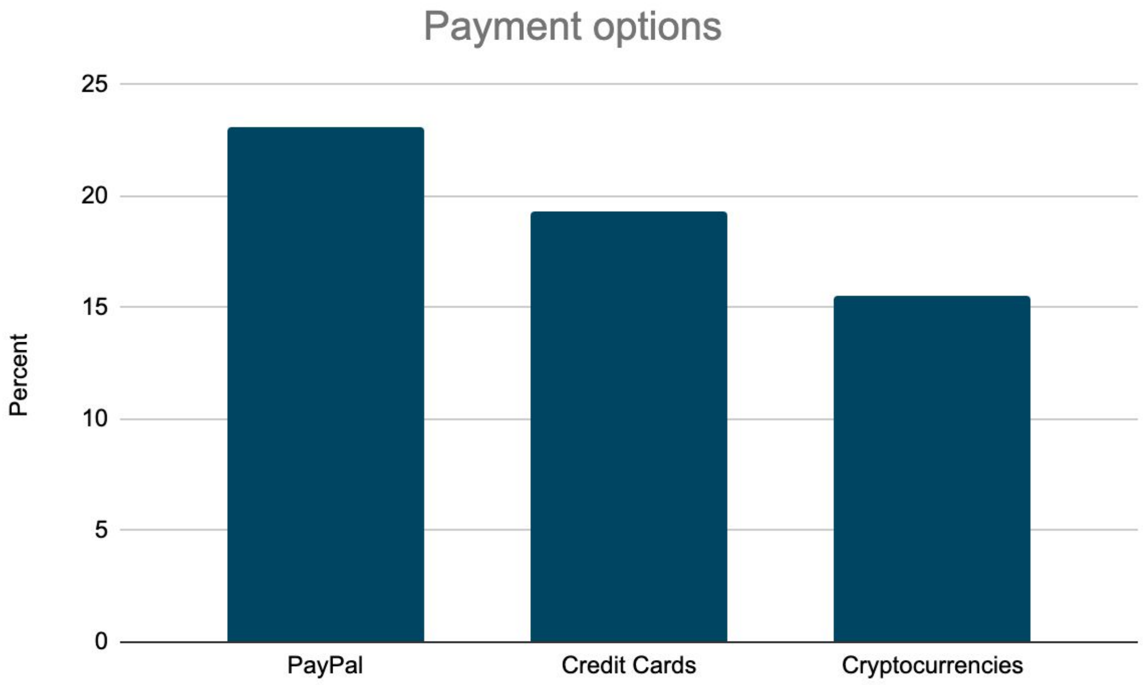


Fig. 6

PayPal, Credit cards and cryptocurrencies are by far the most used payment options by the NCP IPTV blacklist websites, despite efforts from some of these payment providers to block illegal IPTV related use of the services. Some websites offer several different payment options, while others only offer a single option.

Identifying payment options remains a challenge and the fig. 6 numbers are representative but not exhaustive.

Hosting, domain name registration and top-level domain

When it comes to hosting details regarding NCP IPTV blacklist websites, the patterns are similar to those reported in last year's report. Predominant use of Cloudflare's so-called "reverse proxy" application shows that it remains a favourite in the illegal IPTV ecosystem, as it offers a level of resilience against enforcement, by making hiding certain hosting server details possible. In specific cases, the hosting details can be decloaked or information can be obtained from Cloudflare, but this is generally not possible when collecting this data in an automated fashion.

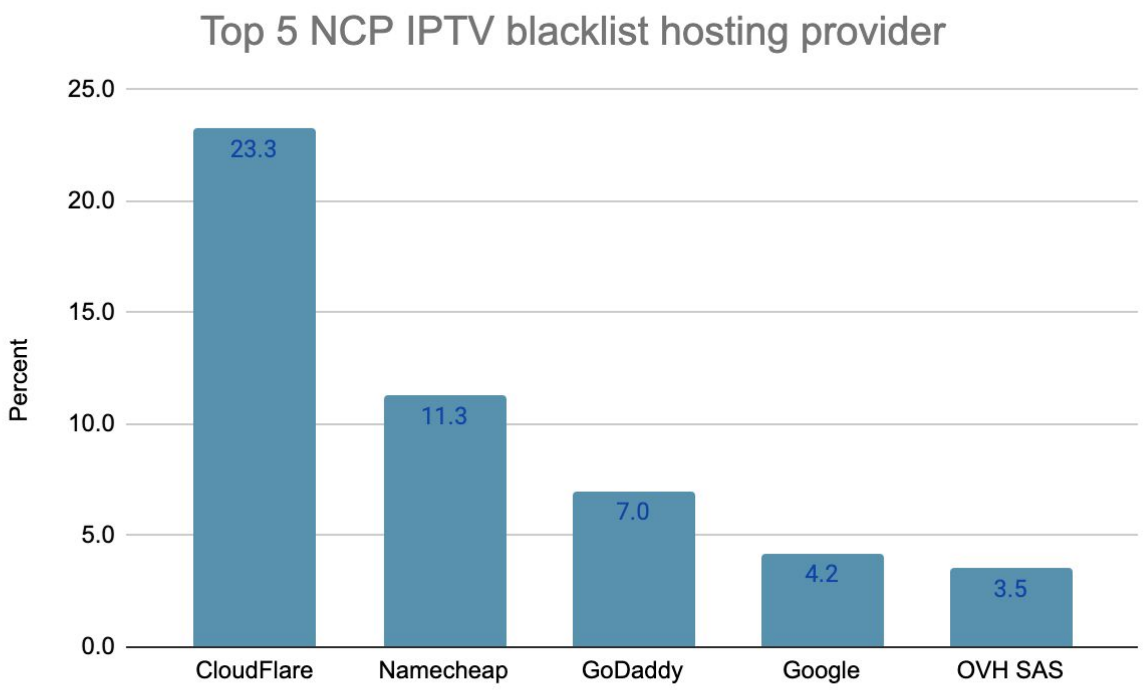


Fig. 7

As Cloudflare is a US-based company, the popularity impacts statistics for hosting countries. However, as several of the largest hosting companies are likewise from the US, we highly anticipate that we would still see the same top five countries as now, even if Cloudflare was not part of the picture:

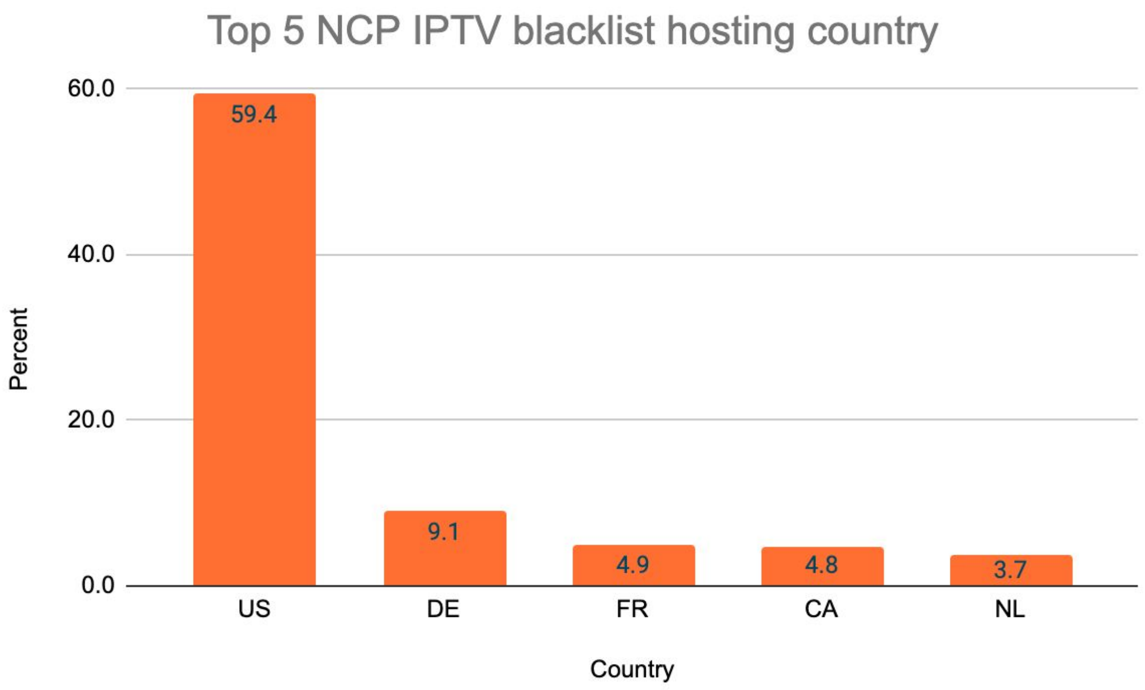


Fig. 8

Further data related to the NCP IPTV blacklist websites is linked to the registration of the domain names. This process is carried out by choosing a free combination of domain name and top-level domain.

> Nearly all NCP IPTV blacklist websites incorporate “IPTV” in the domain names for obvious reasons. Additionally, the domain name will be made further descriptive by adding geographic indicators like country names or entire regions. An example could be “nordic-iptv”.

When this selection is done the domain name has to be registered. This can be done through several different services, but the most common is to use a registrar that charges a fee for the registration. The registrar will finalize the registration and hand over the necessary details to the customer. The process is completed online and registrars traditionally offer the most common online payment options. An increasing number of registrars have been observed to accept Bitcoin as payment.

Below is the most popular registrar services as well as the most popular top-level domains used by the NCP IPTV blacklist websites:

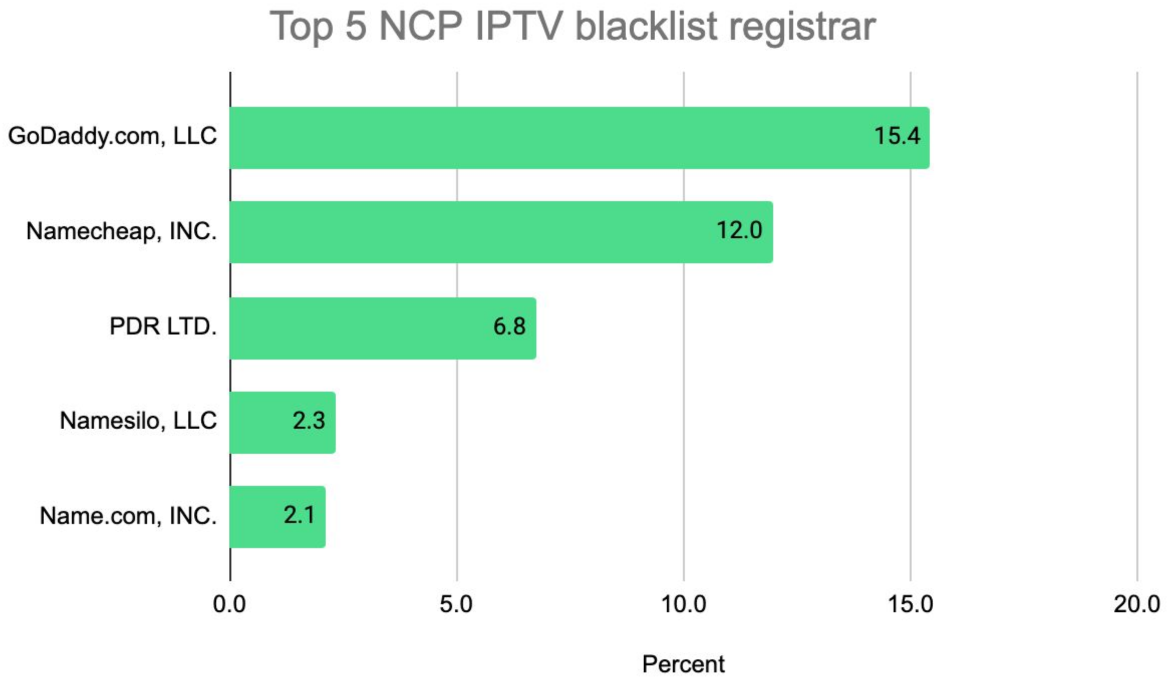


Fig. 9

Not surprisingly, some of the largest registrars worldwide are represented in fig. 9 as they are very popular due to the high level of service combined with low prices. Registration of a domain name costs $10-15 on average for a 1-year registration.

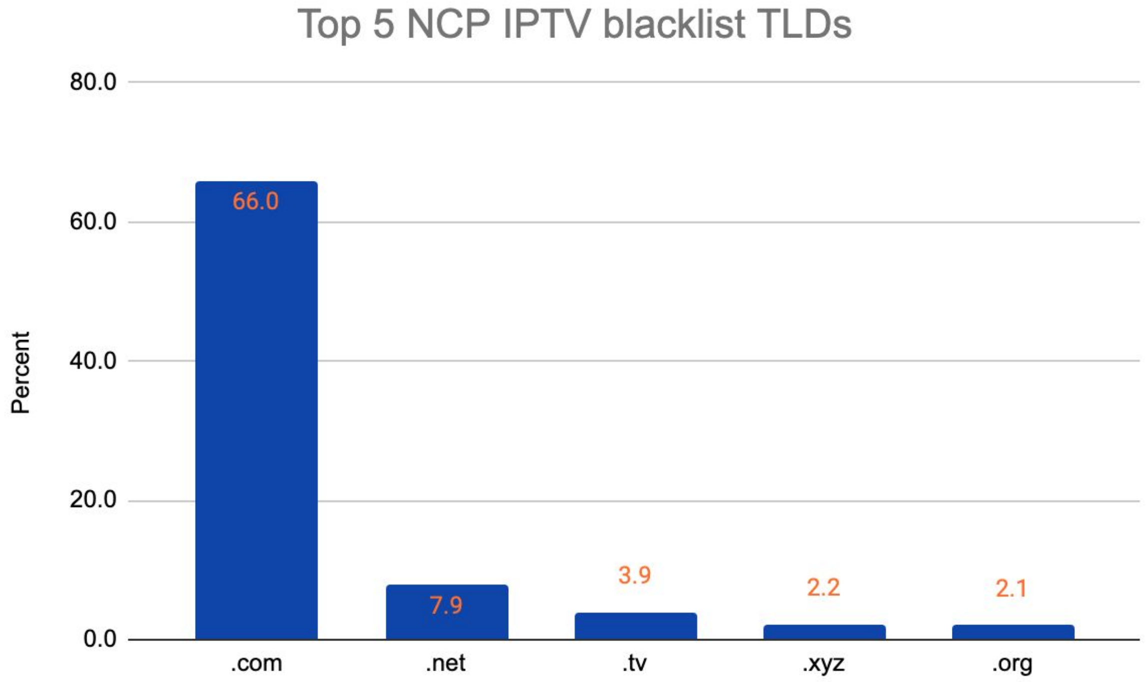


Fig. 10

Compared to last year's report, we have seen the generic top-level domain .xyz replace .info. The remaining statistics are almost identical.

Challenges do remain within the domain name space. Especially regarding whois records. These have been rendered more or less obsolete to their purpose, as EU GDPR regulation has resulted in domain name registries opting to remove whois record details from being publicly available. As a result, the whois part of the DNS system is effectively no longer working and information about domain name ownership is not available.

Social media

Facebook

Another element adding greatly to the current increased popularity of illegal IPTV is social media, which allows illegal IPTV providers to reach and interact effectively and without costs with potential customers.

Although the sale of illegal IPTV is carried out on a number of different social media platforms, Facebook is easily the most popular. Facebook pages are mainly used to promote the illegal IPTV services and attract customers to the dedicated websites described above. Facebook is also used to provide support to and build communities for existing customers. This is often done in closed groups, where admittance depends on the status of being an active paying customer.

NCP monitor Facebook for illegal IPTV providers. Detection of patterns and affiliations enable us to identify which NCP IPTV blacklist websites corresponds to which Facebook pages. The result has enabled NCP to identify connected Facebook pages for more than 24% of the NCP IPTV blacklist websites.

> Identified Facebook pages related to illegal IPTV have a total of 1.3 million followers and have received more than 1.2 million likes.

Facebook provides tools to have infringing content removed from the platform. The use of the tools is generally ineffective, as they mainly consist of pre-set forms, which has to be filled out manually.

Throughout 2019 Facebook has increased its efforts in removing content related to illegal IPTV substantially. And despite some remaining challenges of having infringing content swiftly removed from Facebook, NCP is constructively working with Facebook to improve the efficiency of this matter.

The economic impact of illegal IPTV

2017 numbers

Illegal IPTV is a very lucrative form of crime. In our annual report of 2017, we produced a set of economic estimations based on the anticipated number of active customers in the Nordic countries. Our estimations covered illegal TV as a whole, including both customers of illegal card sharing networks and illegal IPTV.

In total, we estimated that the Nordic region (SE, NO, FI and DK) comprised a total of 400.000 illegal customers. Based on this, we calculated the following

- Illegal annual revenue of nearly €80 million.
- Annual legal earning potential for the Nordic TV industry of €531 million.

2019 numbers

In November of 2019 EUIPO published a research report[2] about illegal IPTV as part of the overall project concerning online business models infringing IPR.

The report conducts a “quantitative analysis of suspected illegal IPTV in the EU”, which, similar to the 2017 annual NCP report, aims to estimate the magnitude of illegal users and the corresponding illegal revenue. This is done for all 28 EU member states and the results are based on 2018 numbers.

As noted in the 2017 annual NCP report, Sweden has more illegal IPTV providers and customers than the other Nordic countries. This is confirmed by the 2019 EUIPO findings that calculate that 8.5% of the Swedish population consumes illegal IPTV. This is the second-highest number in the EU only surpassed by The Netherlands. For Denmark and Finland, the numbers are respectively 5.8% and 4.9%. Norway is not part of the study.

For all 28 EU member states, EUIPO calculated:

- A total of 13.7 million (3.6% of the EU population) access illegal IPTV.
- A total of €941.7 million in annual illegal revenue.

The total sum of annual illegal revenue for Denmark, Finland and Sweden amounted to €85.7 million.

[2] Illegal IPTV in the European Union, EUIPO, November 2019.

As Norway was not covered in the study, we have used the results for Finland, which is comparable in size of population, in fig. 11 below to calculate the collected illegal revenue for the Nordics to be:

- €102 million.

Which amounts to a 31% increase in two years, when compared to the 2017 NCP estimations.

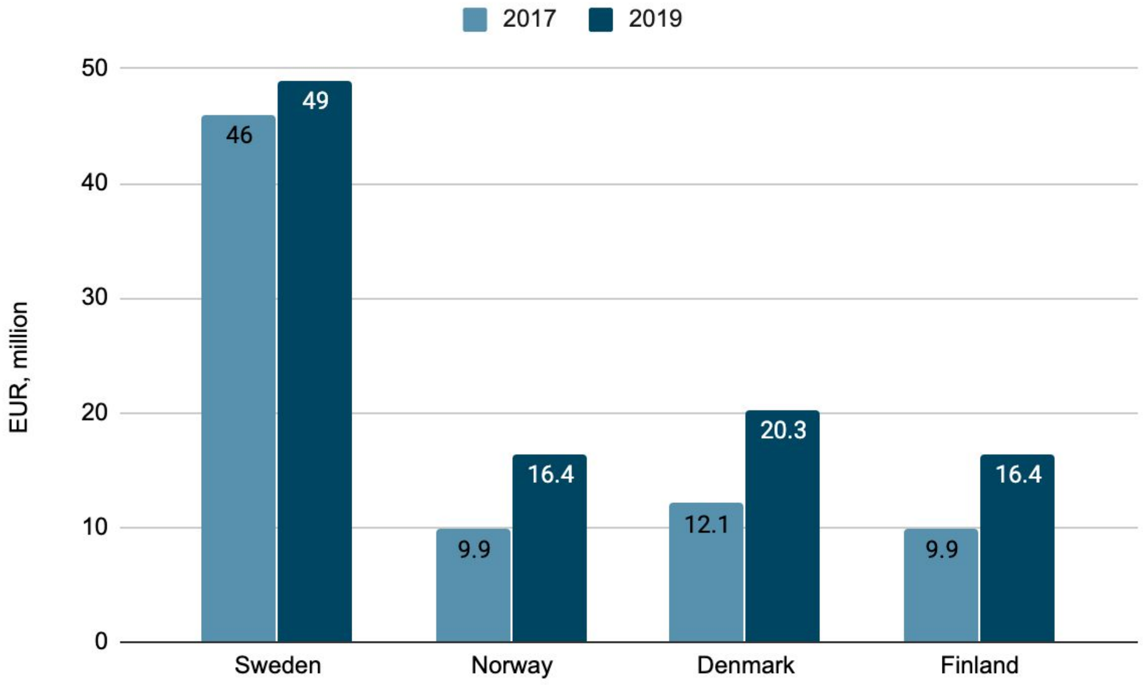


Fig. 11

Enforcement

It is a busy time working with enforcement for the Nordic TV industry. The number of individual illegal IPTV providers is very high and rising. Countless infringing videos are added to Youtube and similar platforms on a daily basis and many of the involved Internet intermediaries are not geared to assist in timely enforcement actions.

Luckily a large set of enforcement tools are available, and many of them are effective. Yet, to be able to tackle the massive problem of TV piracy effectively, prioritization of the most imminent threats as well as the most impactful activities must be given.

Interventions such as website blocking and domain name suspension might only have a limited effect, if the criminals simply register a new (similar) domain name and relaunch the infringing website from a backup. Conversely, a focused effort against illegal IPTV streaming infrastructure such as authorization- and streaming servers is likely to be very effective, as it impacts customers directly, who will experience a flawed service.

Investigations and subsequent criminal cases against illegal IPTV resellers are always relevant, but removing a couple of resellers and disrupting their services might only have limited effect, as they are unlikely to control significant streaming infrastructure nor do they have that many customers. A case against LSPs requires more resources and is often extremely complicated to investigate. A coordinated and successful operation, however, will have a substantial impact on the illegal IPTV ecosystem.

Xtream Codes operation - successful enforcement example

As a result of a four-year-long investigation, Italian and other national police forces carried out raids against an international criminal network providing illegal IPTV. Part of the operation was a raid against Xtream Codes, which for years has provided the most prominent and popular software for setting up and running illegal IPTV businesses[3].

More than 200 servers in three countries were taken offline in addition to 150 seized PayPal accounts. In total, more than 20 suspects were identified.

The case is expected to have impacted more than 700.000 customers of illegal IPTV, and by monitoring discussions in relevant affected communities there is no doubt that many frustrated customers of illegal IPTV were deterred and turned to legal providers of TV.

As an example, this case illustrates how a large, resource-consuming and complicated case can have maximum impact on the criminal business models of illegal IPTV.

Perspectives

NCP expects the threat of illegal IPTV to continue to increase. But we will keep up. By continuing to develop novel investigation techniques and intelligence gathering systems, we will ensure that adequate monitoring is taking place. We will utilize our knowledge to assist the TV industry and our partners in focusing our combined efforts towards actions that have the highest possible impact.

[3] https://torrentfreak.com/xtream-codes-iptv-system-targeted-in-massive-police-operation/
http://www.eurojust.europa.eu/press/PressReleases/Pages/2019/2019-09-18.aspx

Within law enforcement there is a saying that goes: “it takes a network, to defeat a network”. It refers to the challenges of investigating advanced criminal networks that operate across borders. This can only be done through cooperation and well-established networks. In this case between the TV industry and law enforcement.

NCP is committed to maintain and further develop our already excellent cooperation with Nordic and European law enforcement agencies as well as prosecution offices. We intend to continue to provide cases as well as intelligence data to support authorities in understanding this form of crime at the highest level. We also continue to prioritize to assist with training of investigators, prosecutors and judges on both national and international levels, as this is a crucial part of ensuring that cases against TV piracy are handled at the best possible level.