NORDIC CONTENT PROTECTION

CASE STUDIES 2018

Nordic Content Protection

NORDIC CONTENT PROTECTION

% Accounter
Herlev Hovedgade 195
2730 Herlev
Denmark
www.ncprotection.com

Introduction

This is the third annual report published by Nordic Content Protection (NCP) and compiled in December 2017.

Instead of continuing with our usual Trend Report format, we decided to focus the attention on two actual criminal cases, previously reported to law enforcement by NCP. The decision to change the topic, was primarily based on the intention to provide further insight into the work NCP conducts (with regards to enforcement of intellectual property rights) than is possible with the more standard yearly report.

Describing investigations and case events is always a considerable challenge, and a fine balance between providing a sufficient account of the events, without disclosing too much detail in terms of investigational techniques used, whilst continually respecting the right to privacy. For this reason, some aspects of this report have been intentionally omitted.

Readers with relevant and valid inquiries about specific details, are welcome to contact NCP for further information and knowledge sharing.

The report will conclude with a final section on the current threat landscape, as we have previously witnessed unfold in 2017.

Table of Contents

About NCP

NCP aims to prevent illegal access to television content received via satellite dish, digital or analogue terrestrial transmissions, IPTV, cable transmissions, and streaming via Internet.

The NCP organization consists of experienced high-tech, and professional crime investigators with a proven track record in Nordic law enforcement, in combination with technical specialists.

NCP is jointly working with the following Nordic and international distributors, and rights owners as of January 2018: -

NCP is continually co-operating with content distributors to further develop security solutions aimed at detecting and preventing illegal TV content distribution. NCP has a number of additional tasks related to training, and exchange of skills, both nationally and internationally. Current collaborators in these areas include Police IPR[1]-units in Sweden and Denmark, Europol (in advanced computer forensics), the EU, through EUIPO (European Union Intellectual Property Office), and TAIEX4 (Technical Assistance and Information Exchange) workshop.

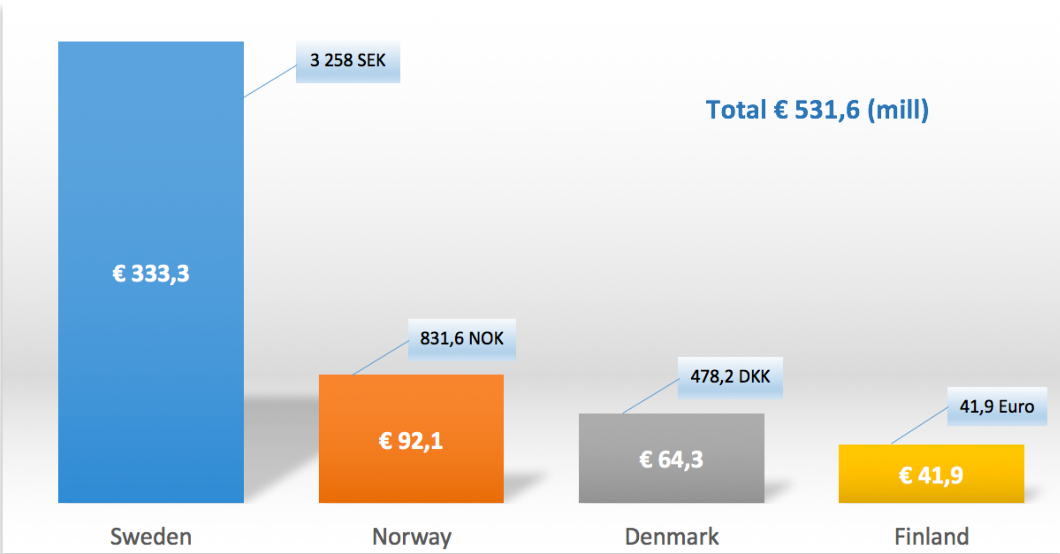
Further information about our work can be found by visiting our website at: www.ncprotection.com

[1] Intellectual Property Rights

Summary of Trend Reports 2016 & 2017

To provide insight and perspective to this report, we have highlighted a few of the main trends and findings from our previous reports below: -

> *"Television piracy remains a highly lucrative, white-collar crime. Three main platforms constitute the main threats to legal TV right holders. These are Card-Sharing[2], IPTV[3] and streaming[4], and they all benefit from the technological developments of recent years, not least the higher Internet speeds. The number of illegal IPTV distributors is increasing rapidly, with the main sales taking place on dedicated websites on the open Internet".*
>
> *"NCP estimate a total of 400.000 illegal TV subscriptions in the Nordic countries of Sweden, Denmark, Norway and Finland[5]. Resulting in a yearly turnover of approximately 80 million Euros for the distributors of illegal content".*
>
> *"Theoretically speaking, if those 400.000 customers of illegal distributors were to become official paying customers of legal distributors, they would represent an earning potential of more than 530 million Euros".*



Estimated earning potential of legal TV distributers in the Nordic countries – NCP Trend Report 2017

[2] Card-sharing is a method by which independent receivers obtain simultaneous access to pay television services, using one legitimate satellite TV smart card (http://www.aapa.eu/about-aapa/piracy-card-sharing).
[3] IPTV (Internet Protocol Television) is delivery of TV services via the Internet. Infringing IPTV is most often sold as subscriptions of varying lengths (i.e. 1, 3, 6 or 12 months) with a large number of channels including premium channels.
[4] Streaming in the context of this report, is streaming of TV channels for example; live sport events, where the content is presented on a website in an embedded media player.
[5] NCP Trend Report 2017

"Despite the massive scale of the underground economy involved with TV piracy, it unfortunately remains (by and large) a low priority for Nordic law enforcement. Authorities both in Sweden and Denmark specifically are strengthening their efforts in recent years, but only regarding cases often being reported to them by NCP, or other industry stakeholders. This is largely the main reason why TV piracy currently remains a low-risk crime which (in combination with the high-earning potential) makes it extremely lucrative to organized crime groups".

"Based on the highlighted trends and findings, NCP estimate that TV piracy will continue to increase dramatically in the number of providers over the coming years".

Case Studies 2018

As an example of the procedural approach of investigating and working on a criminal case from start to finish, we have used a sequential method, which is divided into the following sub-sections: -

- *Case initiation (process of opening a new case)*
- *Preliminary investigation*
- *Main investigation*
- *Case conclusions*

This method allows us to highlight our considerations, decisions and challenges for each of the two described cases.

We have chosen a card-sharing (CS) case from Sweden as the first example, which we will call "***CS Case Sweden"*** throughout the report. Our second choice is an IPTV case from Denmark, which we will call "***IPTV Case Denmark"***.

Case initiation

NCP quite often initiate cases based on our own intelligence, which is meticulously gathered from online open sources[6]. We maintain a close relationship with all our members and partners, who frequently assist in highlighting new or developing threats. Furthermore, NCP operates a hotline service via our website (www.ncprotection.com) where individuals or organizations can tip us (or report) of illegal activities, or indeed any other relevant information.

> Test purchases are an effective means of investigating potential crimes, in allowing the investigator to gauge the true extent and scope of the crime, as well as provide technical evidence and solid intelligence.

For users of the hotline service, anonymity is optional.

"CS Case Sweden" commenced in October 2011, when an anonymous person contacted NCP in Sweden, and offered to sell us a Dreambox[7], which he had in his possession. The Dreambox was directly connected to a card-sharing server[8] with full access to Swedish pay-TV channels. The person was oblivious to any information about the card-sharing network, or indeed the parties running it.

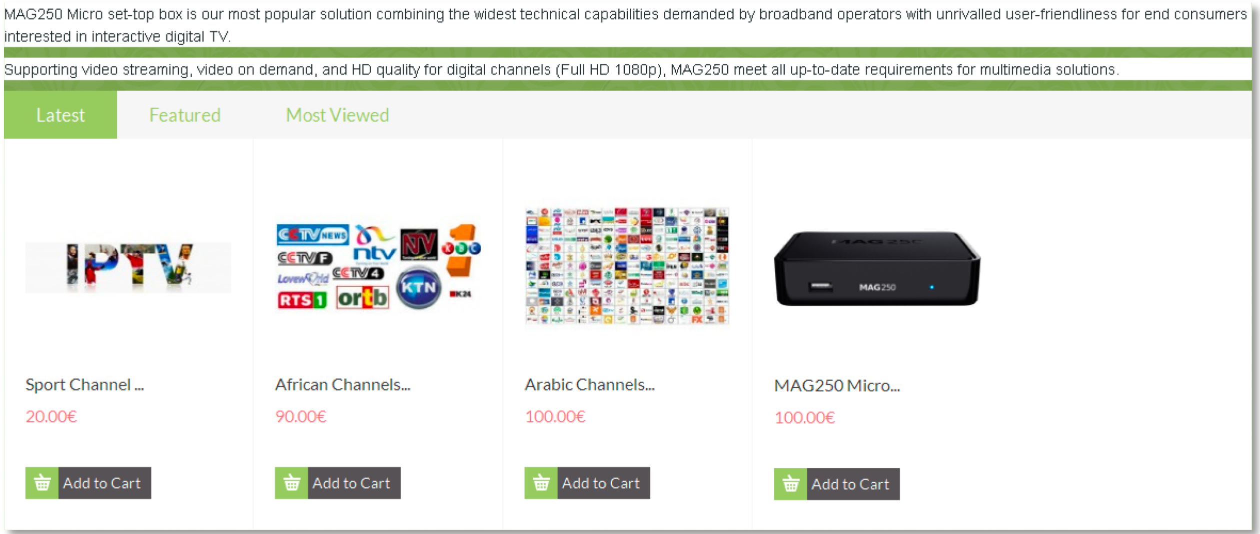
NCP opted to purchase the Dreambox for 3500 SEK (approx. €350) which was paid in cash in person. Subsequently the Dreambox was tested and analysed shortly after we received it, con-

[6] Open sources represent information and data publicly available on the Internet.
[7] A Dreambox is a multipurpose set-top box, which can be configured to behave (function) as both a card-sharing client and server.
[8] A card-sharing server is a key part of a card-sharing network, as it facilitates decryption and sharing of control words, as well as connects to other servers and receives control words from them enabling access to other channels without a legal subscription.

firming that it did actually provide illegal access to almost all Swedish TV channels (including all the popular premium channels) through a functioning card-sharing network[9].

"IPTV Case Denmark" had a similar start, where an informant (who also chose to remain anonymous) established contact with NCP Denmark. He initially approached us in May 2014. He offered to hand-over an IPTV set-top box that he had previously purchased, as well as supplying information about the website which sold the item.

NCP accepted to acquire the box, which subsequently was delivered by mail shortly afterwards. As a result, NCP was able to gather sufficient information from the illegal website, who initially sold the set-top box named MAG 250[10] for €100, and a Sports channel package for €20 per month. A detailed channel list on their website revealed that three Nordic channels were also included in the illegal subscription.



Above: Actual website snapshot image.

Before considering taking on a case, NCP formulates the best chances of success, and evaluates the potential risks factors. These precautions are necessary to ensure that resources are used efficiently to the highest potential benefit of the NCP members, as well as the overall goal of reducing the threat of TV piracy.

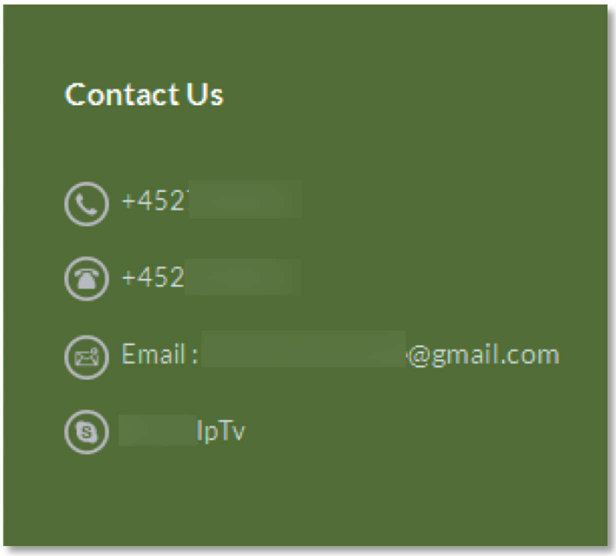
Preliminary investigation

Immediately after deciding to take on a case, the initial investigation phase commences. The point of this phase is to ensure that all data (which might serve as evidence) is fully documented and taken into account for evaluation. The same rules apply for website, and social-media content, alongside available log files, communication via e-mail and more.

[9] A card-sharing network is a network of clients and servers, where decryption and sharing of satellite TV signal control words takes place to enable illegal access to pay-tv channels.
[10] The MAG250 set-top box is manufactured by Informir https://www.infomir.eu/eng/products/archive/mag-250. The MAG250 needs to configured, post production, to access illegal IPTV content.

For ***"CS Case Sweden"*** no further documentation or data collection was required, as the Dreambox was not purchased on the Internet. The box was subsequently tested to see whether access to Nordic channels were available. This was later confirmed by NCP, and connections to three individual Internet domain names, were identified through the device, which were *all* hosted by Swedish Internet service providers (ISP).

In ***"IPTV Case Denmark"***, we immediately documented a variety of information that was available online, which we believe could assist in the identification of the alleged suspect or group of suspects, as well as illustrate the full scope of the crime. This included website layout, contact information, and details pertaining to the products being offered for sale on the website.



Contact information – (details intentionally blurred)

The offending website contained a valid Danish phone number and an e-mail address as contact information. The top-level domain name[11] used in the e-mail address, corresponded to the name of a company registered with the Danish Company Registry[12].

In both cases, it was absolutely clear that the rights of Nordic TV content providers were directly violated, as the set-top boxes provided unauthorized access to Nordic channels. In addition, there were indications that the alleged suspects were presently located in Sweden and Denmark respectively.

Main investigation

Entering the main investigation stage, NCP planned a strategy for the remaining case (with the co-operation of relevant members or partners). Thorough information gathering, and continuous monitoring were also essential parts of this phase. In some cases, there was a need to interact covertly with alleged suspects either to identify them, or to further understand the scope of their criminal activities.

[11] A top-level domain (TLD) is the domains at the highest level in the hierarchical Domain Name System of the Internet.
[12] https://virk.dk

Main investigation, CS Case Sweden

In ***"CS Case Sweden"***, the final analysis of the Dreambox was carried out and systematically documented. This particular case revealed that the available Swedish TV channels belonged to a specific Swedish cable TV provider.

As previously mentioned, the Dreambox configuration prompted it to automatically connect to three specific Internet domain names (usually authorization servers or update servers) when it was powered on. The servers hosting these domains were part of the card-sharing network, and therefore very relevant to the case. By using publically available Internet registries, NCP was able to ascertain that those domain names were hosted at servers located in Sweden.

The final observations were established: -

Domain 1: was hosted by a company located in Stockholm, offering web hotel services.
Domain 2: was hosted by a hosting service provider offering anonymous hosting.
Domain 3: was hosted by a major Swedish Internet service provider (ISP).

NCP utilized intelligence data gathering techniques through online open sources about card-sharing networks, to estimate how long this network had been operating. In addition, frequent network lookups were initiated to monitor and detect intermittent network infrastructure changes.

> Whenever NCP reports cases to the authorities, we aim to provide specific house search and interrogation guides tailored to each and every case. This is to ensure that the law enforcement personnel have access to best practices and technical knowledge whilst they carry out their investigations and subsequent operative actions. We are able to provide this complimentary support because of our wealth of professional industry knowledge, expertise and our background as police officers with technical training and education.

In collaboration with the NCP members, we finalized the reports required to hand over the case to the Swedish law enforcement. This was completed in May 2012. In October 2012, Swedish Police carried out the first house search, which related to Domain 1.

Besides the NCP case, the Police had other on-going cases against the server in question.

The card-sharing server was successfully identified and seized by the Police during the search. However, it appeared that an employee of the web hotel company, publicly used Twitter to announce that the Police were present at the company address. This was something not foreseen, and actions like this could result in a negative effect on the outcome of the Police actions.

NCP is continuously committed or actively engaged in a variety of training sessions with police investigators, prosecutors and judges across the Nordic countries and EU. We prioritize this aspect of enforcement support, as we firmly believe that the higher the authority skill level, the higher case quality and success rate. This benefits everyone and ensures that resources are utilized in the most efficient and best way possible.

In early 2013, NCP was asked to assist the Swedish Police with knowledge on how card-sharing networks function and operate. We have since learnt that the confiscated server had been erased prior to the seizure, and only a small amount of relevant data was retrievable by the forensic investigators.

Continuing the investigation, the Swedish Police attempted to obtain information from the major Swedish Internet service provider hosting Domain 3. Unfortunately, no information leading to identification of a suspect was available.

Though NCP was never officially informed about the detailed circumstances surrounding these particular events, we understand that a specific network switch at the location of the Internet service provider had been tampered with, resulting in no available evidence as to whom was responsible for operating the illegal server, and who precisely were the customers/users.

The Domain 2 server, which made use of anonymizing services to hide its IP address[13], (a tactic quite often adopted by the criminals) remained the only option for further investigation. NCP assisted the Police by in-depth probing of the services provided by the company behind them. From this analysis, we since learned that the anonymizing technology was flawed, and would occasionally disconnect, thus momentarily rendering the actual IP address of the server visible.

In the hope of exposing the hosting information for the Domain 2 server, NCP kept monitoring the domain. Unfortunately, the Dreambox subscription expired, thus we could no longer confirm whether the card-sharing network was still active. This resulted in a decision by Swedish Police, to end the investigation, since they had no more viable leads to pursue.

By the end of 2014, the Swedish Police was no longer investigating the case. NCP re-examined the case and identified that only Domain 3 remained active at this particular time.

Then in the beginning of 2015, NCP was informed about an external organization, which was directly connected with a NCP member. Some of the organization staff apparently used card-sharing services. Initially this information was completely independent from the case, and NCP decided to physically visit and meet with the organization. This led to NCP having access to several set-top boxes and to different card-sharing networks.

Early analysis proved, that several of the set-top boxes were connected directly to the exact same network as we had previously reported back in 2012. Some subtle changes had been made over time, but the evidence was absolutely clear. This was confirmation that the card-

[13] An IP address a unique identifier for devices communicating via the Internet Protocol.

sharing network was indeed still active and providing illegal access to Nordic pay-tv channels. As a result, NCP submitted a new report and informed the Swedish Police about of our findings.

The main evidence was determined by the continued use of Domain 3. We were able to confirm that the server running Domain 3 was holding a total of three official satellite TV smart cards,[14] and as a result became a vital part of the card-sharing network.

During the **CS Case Sweden** investigation, NCP approached several companies who provided the anonymizing services. Pointing out what potentially their services could be used for, i.e. the supply of illegal access to pay-TV, successfully resulted in at least one of the providers opting to block all card-sharing network traffic on their systems. This direct contact often yields positive results, and is something NCP frequently utilizes when working with Internet service providers (ISP).

Based upon fresh evidence submitted by NCP, the Swedish Police resumed the investigation with Domain 3 being the main target. In June 2015, they were able to trace the server location to a private apartment in the south of Sweden, which was searched by Swedish Police at this time. During the house search, the investigators noticed that the network installation in the basement of the apartment building had been evidently tampered with. A locked room in the basement revealed a running computer, which was connected to the Internet. Upon on-site inspection, they were able to confirm that the computer was indeed connected to the card-sharing network, which NCP had described in the latest report.

Our determination in pursuing the alleged criminals, along with our persistent investigative skills, led to the eventual capture and arrest of the main suspect, and several other related suspects within the same day.

During the operation, only one server (with the attached official satellite TV smart card) was seized by the Police. Unfortunately, this was not enough to shut down the complete card-sharing network (which still continued to operate). However (continuing their efforts) the Police managed to identify the IP address for the card-sharing network customer login server[15]. This was hosted by a so-called, hostile[16] Internet service provider in Stockholm. They subsequently provided the following explanation about the IP address in question: -

> Quote: *"This IP address, which belongs to us is not officially in use. It belongs to a test Wi-Fi network for a shopping mall in a Stockholm suburb."*

Without the cooperation from the Internet service provider, no further action was possible regarding this illegal server.

---

[14] A satellite TV smart card decrypts satellite TV signals so the content becomes viewable.

[15] Illegal CS set-top boxes are usually required to connect to a login server, which verifies an active account, a prerequisite to access the illegal content.

[16] The term 'hostile' is used to describe Internet Service Providers who are non-compliant with substantiated take-down requests and/or who incorporate different measures in their business model to ensure that they are not able to hand-over customer information to be used by law enforcement to identify individual customers (such as customer payment information, logon information and more).

The final breakthrough came shortly after the seizure of the remaining server, as the forensic investigators soon discovered that it contained several official satellite-TV smart cards hidden inside the server cabinet. All of these belonged to NCP members.

Working closely with our members, NCP was able identify a pattern emerging around the discovered smart cards leading us, and the police to another suspect.

In total, nearly 20 official smart cards were identified, and shut down simultaneously by the respective NCP members. Finally, three years after initially reporting the case to authorities, the card-sharing network was finally dismantled.

Main Investigation, IPTV Case Denmark

For **"IPTV Case Denmark"** we continued the investigation by focusing on the received IPTV set-top box. The return address and name exactly matched the details from the Danish Company Registry and the labelling text was in Danish. Inside, was a professionally packed IPTV set-top box, with all the complimentary accessories, such as cables and a remote control.

> Cases in terms of illegal IPTV are becoming (in most instances) a common cross-border crime. Website hosting, authentication servers, streaming servers, customer support modules, are very rarely set-up and run solely from within one country alone. This means that to effectively investigate and prosecute these suspected cases, international co-operation is required. NCP, with its personnel background from Nordic and international Police forces, use their established network and understanding of international collaboration to achieve the best possible results in these very difficult and sometimes challenging circumstances.

After connecting the box to the Internet, we were able to identify a connection to an authentication server[17] located in France. Analysing the available channels and the related streaming servers, we were able to establish only one Nordic channel – a premium sport channel, belonging to a NCP member. This channel was later traced and confirmed by our investigators, as being streamed from a server in The Netherlands.

> Illegal IPTV providers are increasingly becoming more sophisticated by taking advantage of the popular social-media platforms to promote their illegal services, and to interact with existing customers. Skype is equally popular among the IPTV pirates, who use it to keep in touch with each other, as well as to offer customer support, and even to sell access to their illegal services.

Additional searches via open sources revealed an active Youtube channel was created with the company name and with IPTV related videos. In one of the videos, a television is filmed, and it mirrors the camera operator, who was the suspect of the case. We also identified another e-mail address and a Skype account, which if required, could be used to identify the suspect.

[17] Illegal IPTV set-top boxes are usually required to connect to an authentication server, which verifies a valid subscription, a prerequisite to accessing illegal content.

Combining the identified details, and the IPTV set-top box analysis, we had accrued sufficient information to report the case to the Danish Police few days after starting it, in May of 2014. Our report also contained specific recommendations regarding a suspect house search and interrogation. As part of the case, NCP requested to be informed of the latest case developments and offered further support to the Danish Police (if required).

NCP's investigator was called-in as a witness in an upcoming court hearing in September 2016.

Case conclusions

When cases about TV piracy enter the final stages, NCP remain available to assist and support law enforcement throughout. We often provide expert testimonies in court, and we represent our members as plaintiffs[18] during the trial. This position allows us to discover the details uncovered by law enforcement, and for us to identify and assess the skill-level of the local police units involved, which we in turn, use to adjust and target our training efforts with them.

When we represent NCP members as plaintiffs in court cases, we do so by being present at the court proceedings. In court, we present the compensation claims based on the case details, such as the extent of the crime and the number of customers. To accomplish this to the highest precision, we calculate and adjust the claims during the trial hearings, to reflect the current proceedings.

With regard to compensation claims, there are distinct differences in practice between the courts of the Nordic countries.

- In Sweden: the question of claims is always part of a criminal court case.
- In Denmark: the question of claims can be included in the criminal case, but is quite often referred to a Civil Court by the presiding Judge.

The result of this means NCP DK will attempt to negotiate the compensation claims either directly with the accused, or via the defence attorney prior to the trial. This procedure often leads to a reciprocal agreement benefitting both parties.

Case conclusions, CS Case Sweden

Based on the mounting evidence, Swedish Police were able to prosecute three main suspects. They were all found guilty in the city court of Stockholm in 2016. Two of the accused received suspended jail sentences, and one received a fine. NCP testified as witness and technical investigator, and prepared the claims used by the prosecutor during the court proceedings. The final claims for damages, presented in the court by NCP, were approximately 20 million SEK, which were accepted by the court as part of the case.

In June 2017, the verdict was appealed both by the Defence and the Prosecution, and thus went to the Swedish Court of Appeal. The guilty sentence was upheld, but the damages were

[18] Entity who brings a legal action against somebody else.

significantly reduced. The court also subtracted the VAT[19] percentage from the damages, further minimizing the total amount. This ruling has since been adopted by other courts, and has been further appealed to the Supreme Court, which permitted the case to be heard in autumn of 2017, and therefore is still pending at the time of this publication.

"CS Case Sweden" was a very complex case, with a set of anti-enforcement measures in place, to try and further obstruct enforcement against a complicated illegal card-sharing network consortium. This is reflected in the timespan covering the case, as it was initially reported in October 2011 and by early 2018, no court date has been set for the final procedures.

During the investigation there were several dead-end leads, and (by all accounts) the case was closed by the authorities (due to a lack of further evidence). Only because of NCP's persistence and professional commitment, was new evidence discovered and the case subsequently reopened.

Nonetheless the case also highlights the positive impact of the IPR unit within the Swedish Police, as they were able to continue with the investigation, and successfully secure convictions of several TV pirates, who were causing substantial copyright infringements to the TV industry.

Case conclusions, IPTV Case Denmark

The case went before the Copenhagen City Court in September 2016, and NCP testified against the main suspect. He had been identified through the evidence provided by NCP.

The technical evidence revealed that the suspect was indeed a reseller of illegal IPTV services, however the case against him did not shut down the IPTV network.

The suspect was accused of breaking the Danish Copyright Law with a maximum sentence of one and a half years of prison. The suspect was found guilty by the Court and sentenced to 40-day suspended prison sentence. The case was not appealed. Given the number of customers were not identified, NCP was unable to present any financial claim on behalf of NCP members in this case.

In Denmark, cases relating to card sharing, illegal IPTV or streaming of live TV, can be prosecuted in accordance with the Danish Penal Code §299b, which carries a maximum sentence of six years in prison.

For a case to be prosecuted by this provision, the crime has to be significant; i.e. facilitation of illegal access to pay-TV to a high number of customers/viewers.

[19] Value Added Tax

Overall conclusions

Based on the cases described in this report, several conclusions can be summarised with regards to the work of enforcing intellectual property rights in the Nordic countries.
Both events in this report, are covered by rules of public prosecution. However, no investigation or prosecution will ever take place, unless reported by the rightful holder (those which either own or have full authorized rights to the content). Simply reporting websites who are actively selling illegal TV services is highly unlikely to yield satisfactory results, in an environment where authorities are forced to prioritize crime, and so-often lack sufficient resources. Our experience is, that cases which are thoroughly investigated, are far more likely to achieve the needed attention and processing of law enforcement with subsequent valuable results.

This is the key reason why NCP (in each instance) takes special care and attention to assess every case based on merit, as to whether it shall be reported to authorities, or if other means of enforcement is possible. Once it has been decided upon to report a case, NCP will be fully committed in the investigating process, producing a comprehensive evidence package consisting of relevant reports, data and guides. This enables the authorities to gain an advantage on an already well-mapped case, and thus minimizing the need of Police resources. In addition, NCP supports the investigation and case finalization until it is finished.

Despite these efforts, cases often take years to finalise, which allow the criminals to continue their illegal activities until practical solutions are found. Regrettably, this results in further damage to the TV industry. NCP's efforts to assist Police and prosecutors through national and international training, and knowledge sharing are an important factor to remedy the current challenges.

Both cases serve as prime examples of successful enforcement, initiated by the TV industry, brought to the courts by the Police, where the actual criminal activity finally stopped, and the responsible parties were subsequently convicted. These cases clearly demonstrate, that the system (despite some setbacks) does indeed work.

As for NCP's role in addition to providing actual investigated cases, its function is to work closely together with our members before and during cases, and to represent them in the question of claiming compensation, and to link co-operation with law enforcement, and the judicial system during case investigation and trials. Not only in the Nordic countries, but also globally.

NCP actively encourages and supports initiatives to enhance the overall efforts against violations of intellectual property rights. One such effort was part of a stakeholder group in Denmark in autumn of 2017, to push for a strengthened effort within the State Prosecutor for Serious Economic and International Crime. The measures taken, persuaded the Danish Ministry of Justice to create an IP Task Force, with an increased level of resources and manpower at their disposal. The IP Task Force will operate for six months (from November 2017) before it is evaluated.

Threat landscape

NCP continue to monitor and analyse the three principle piracy threats to the TV industry, card sharing, IPTV piracy and illegal streaming.

For card-sharing and IPTV piracy, we collect open source intelligence automatically, which is then later analysed and used to further understand the potential threats, and to build significant cases against the most persistent criminals. Sophisticated monitoring techniques allow us to detect behavioural patterns in the development of these areas, which helps us to react and prioritize accordingly, to always protect the interests of the NCP members in the best way possible.

For streaming, we employ a team of dedicated specialist staff, who work actively to report, and attempt take downs[20] of illegal streaming of NCP member's official content (most often live sport events). Despite the fact that the illegal streams mostly come from hostile services, which refuse to react to take down notices, the effort is indeed valuable. It enables us to expose and map the services supporting the criminal setups, which allows for coordinated actions in collaboration with NCP members and other enforcement stakeholders.

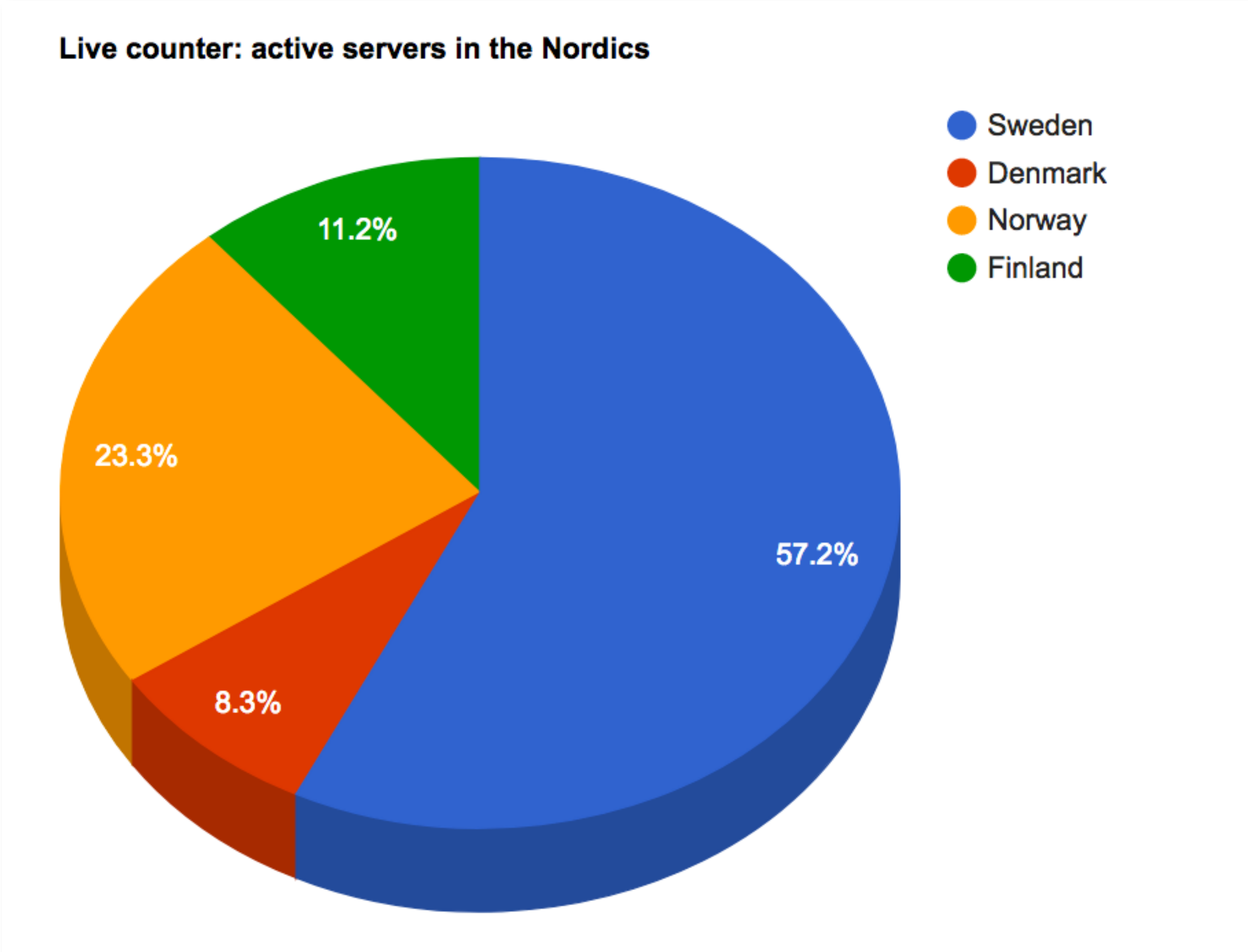
The following sections briefly describe the three main threats and will be supported by relevant statistics: -

[20] Removal of copyright infringing TV content, by means of forwarded take down requests.

Card sharing

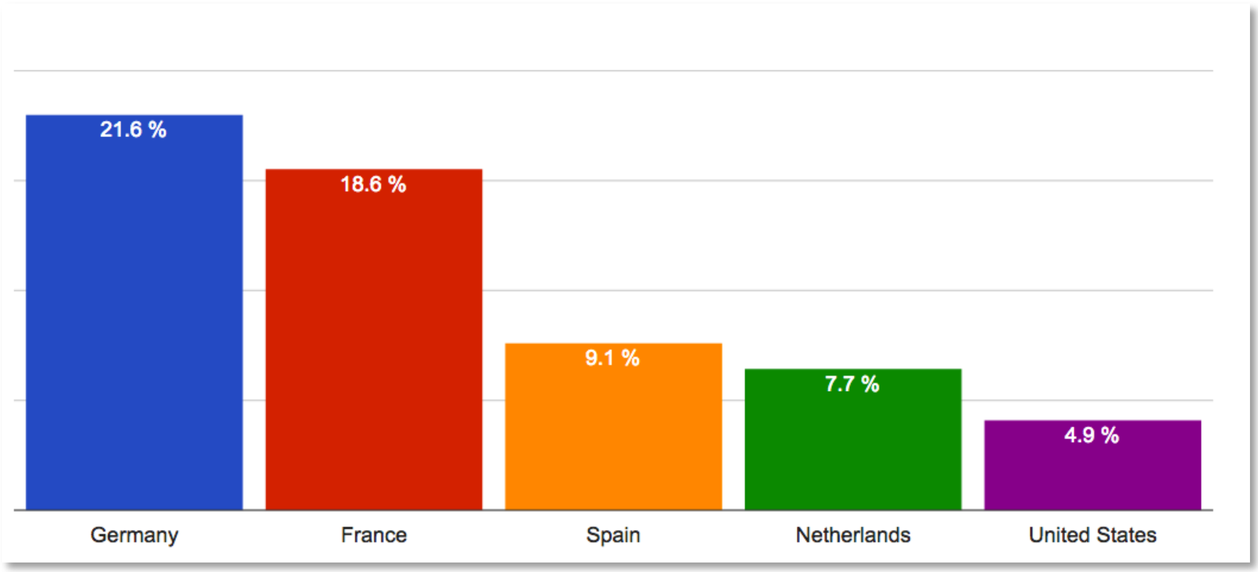
Card-sharing involves at least one, but most often multiple card-sharing servers, sharing official TV subscription cards over the Internet to a number of card-sharing clients receiving satellite TV signals, and thereby illegally accessing pay-tv channels.

Card-sharing servers can be identified on the Internet. NCP focuses on establishing which are illegal servers within the Nordic region, i.e. hosting, Nordic channels or a connection to our Nordic members.



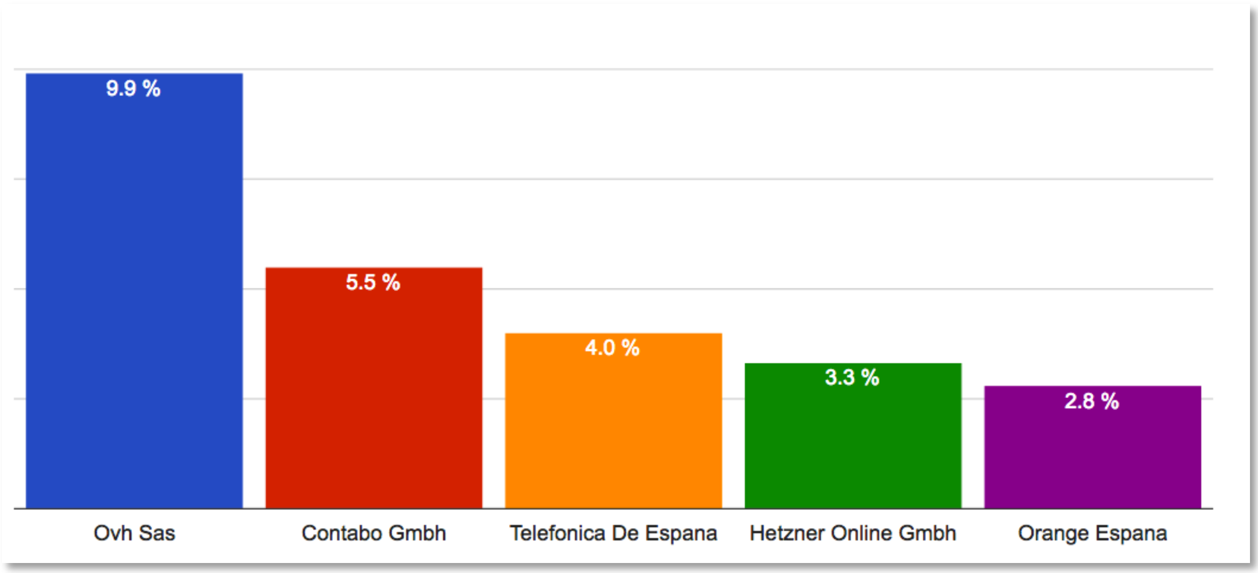
This is the current country distribution of active card-sharing servers hosted within the Nordic countries

When analysing the entire set of known active card-sharing servers the country distribution reveals the following result: -



In 2017, these were the top five hosting countries for card-sharing servers detected and analysed by NCP

Note that mainly European countries are represented here. This is due to the fact that Internet infrastructure is sufficiently developed, and price structure for hosting is (generally-speaking) extremely competitive, thus prices have dramatically reduced over the years. This combination provides sufficient opportunity for the criminals to provide a sophisticated illegal service, with minimum expense.



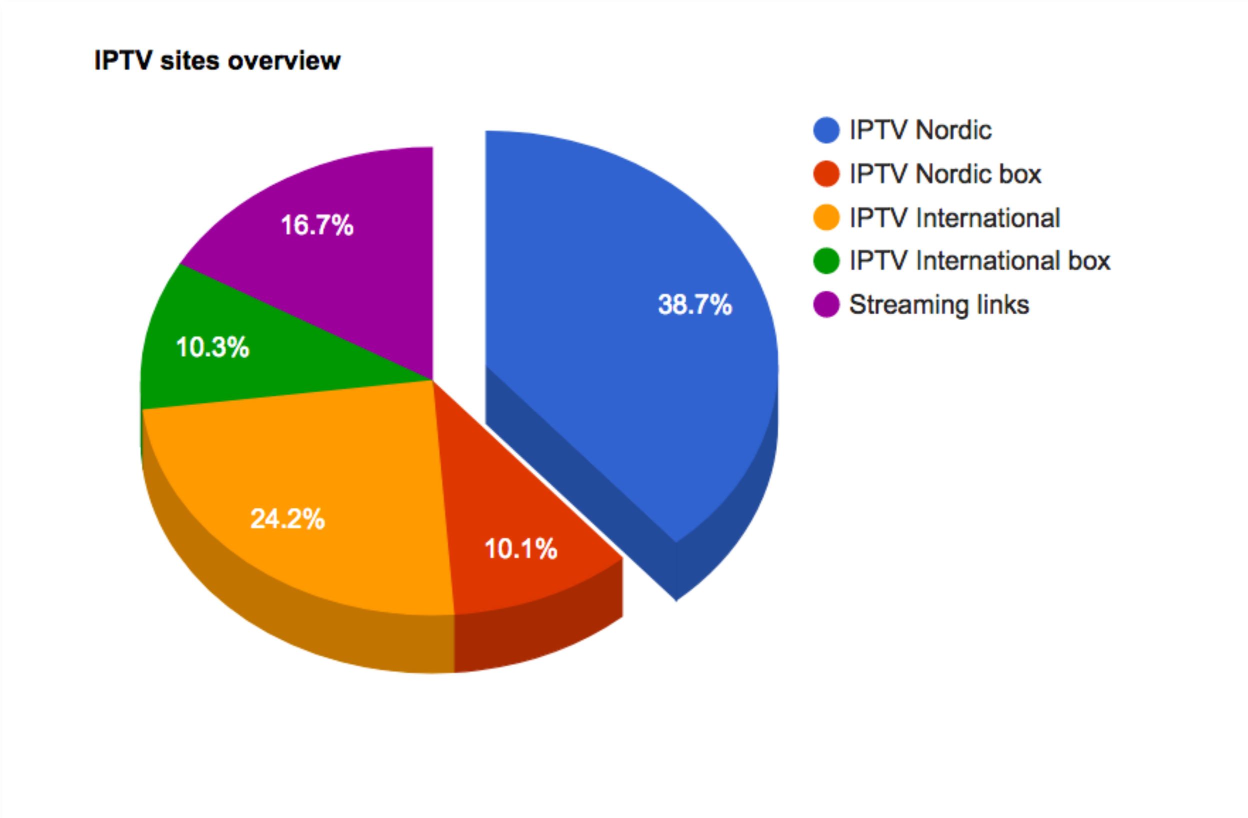
In 2017, these were the main hosts for card-sharing servers detected and logged by NCP

IPTV

NCP has gathered intelligence throughout 2017, on more than a thousand websites offering illegal IPTV subscriptions. As in the case with card-sharing, NCP focuses on detecting and logging websites with a Nordic footprint. By creating and using specific web scrapers[21] and scoring algorithms[22], we are able to detect relevant websites shortly after they become illegally active.

After automated detection and prioritization, each website is manually categorized to ensure the highest possible quality of the gathered intelligence.

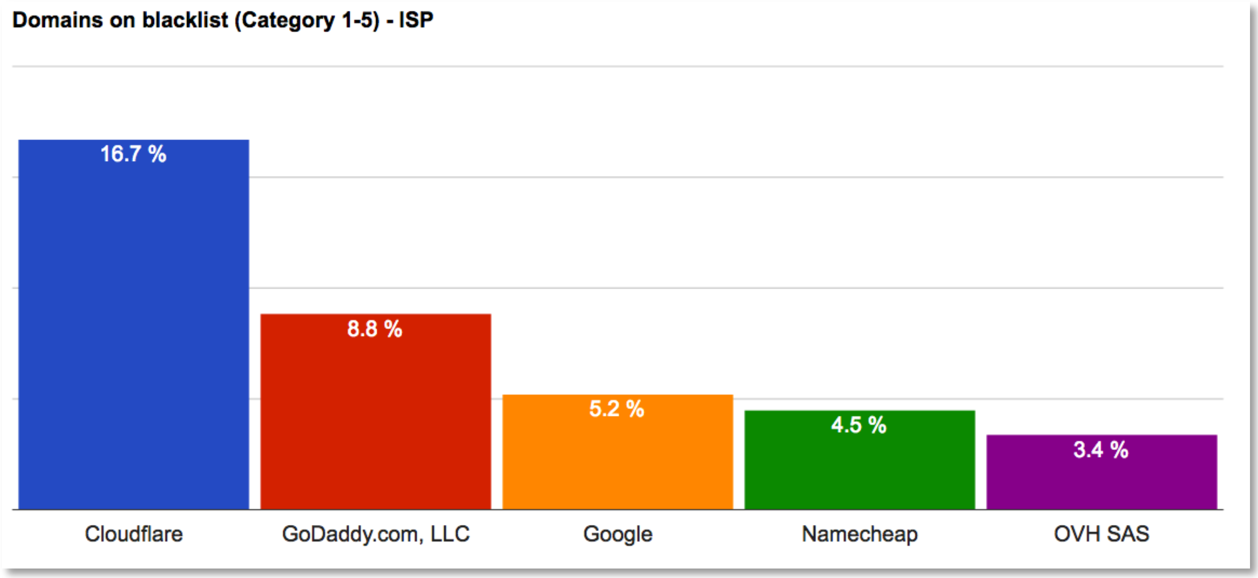
The following illustration represents the current status in early 2018: -



Category 1-4 covers websites selling IPTV subscriptions (with or without Nordic channels and set-top boxes) while category 5 covers streaming websites

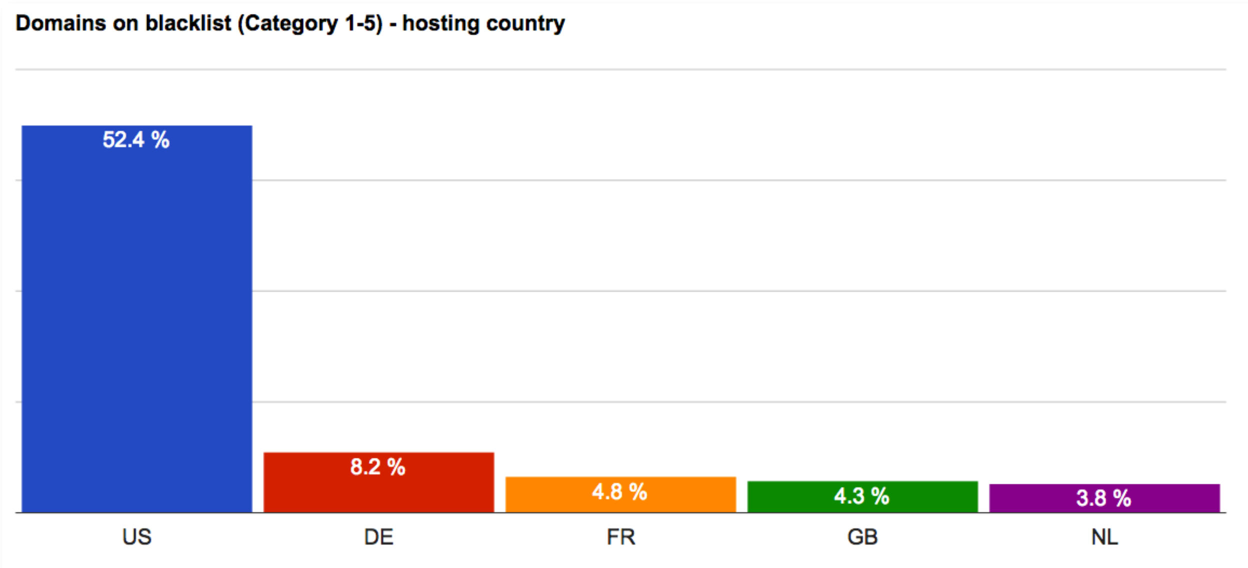
[21] Specialized software capable of both detecting and documenting specific online information.
[22] Software able to calculate illegal impact via a pre-defined website data evaluation system.

Based on the gathered intelligence we are able to extract the following statistics regarding illegal IPTV websites:



Hosting (or CDN's[23]) providers for websites selling IPTV subscriptions

Hosting of the illegal IPTV websites takes place in the following countries:



Hosting countries for websites selling illegal IPTV

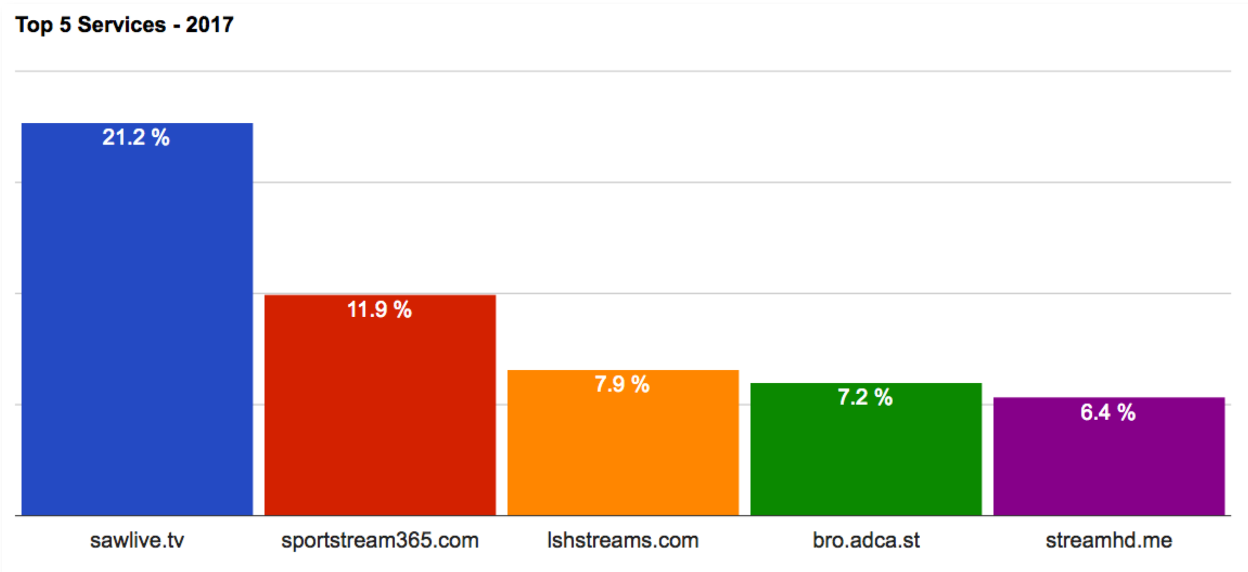
Note: indications that a significant proportion of the illegal IPTV websites were apparently hosted in the US is considered as inaccurate, as many were found to be subscribing to Cloud-Flare[24] services. Therefore, the statistical data must be considered as a false representation of websites being physically hosted in the US.

[23] Content Delivery Networks.

[24] CloudFlare is an American company offering a range of Internet services. One CloudFlare service acts as a 'reversed proxy', which allow website hosting details (DNS) to point to CloudFlare network infrastructure instead of the actual point of hosting, effectively hiding those details.

Streaming

NCP has been instigating take down requests on live streaming content since 2014. Initially the success rate of removing infringing streams was about 50%, but the criminals has since realised that use of legitimate services often result in removal of their illegal streams through take down notices. NCP's long-term campaign is partly responsible for this outcome, and the consequence has been that the criminals have since moved their illegal activities to so-called hostile services, which do not comply to take down notices. As a result, the "removal rate" has since been significantly reduced.

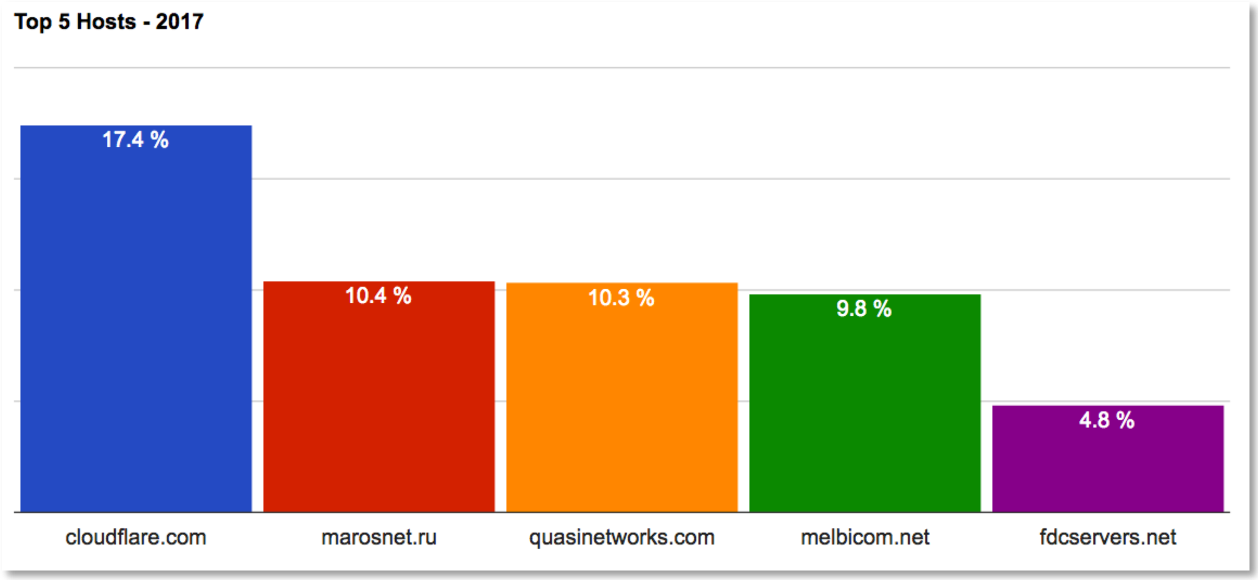


In 2017 these were the most frequently used hostile services to facilitate illegal live streaming of TV content

NCP sent more than 1500 take down notices throughout 2017 to identified services (including those in the above graph) facilitating illegal live streaming of NCP member content.

For each infringing stream of content, the IP address from where the stream originated from was identified. The services utilizing those IP addresses were then notified automatically once per month about the infringing streams and requested to remove such illegal content.

The top 5 of these services were: -



In 2017, these were the main services providing network infrastructure which were used to illegally stream live TV content