Nordic Content Protection

Trend Report 2016

Criminal developments in illegal distribution and selling of illegal access to television broadcasts

This trend report is a collaboration between the analysis and consulting company Procope AS and Nordic Content Protection. Oslo, December 4, 2015.

PRO/COPE

Table of contents

Summary

Illegal access to television broadcasts through cardsharing, streaming and IPTV constitutes a serious threat to legal distributors[1]. Illegal access costs the industry an estimated 4 billion NOK annually in lost revenue. In the Nordic market, criminal operators turn an annual profit of 600 million NOK. Criminal court cases reveal that individuals have accumulated sizeable fortunes through these illegal activities. In other words, this avenue of illegal endeavor is extremely lucrative and carries a low risk of detection and prosecution.

This form of criminal activity has by and large escaped public interest. Positive developments are, however, taking place in the field of law enforcement. Noteworthy initiatives include the establishment of IPR-units (Intellectual Property Rights) in Sweden and Denmark. The IPR-units have already made contributions in several cases with positive results. For the time being, no such task force exists in Norway or Finland.

The main threat to the industry is the high number cardsharing networks, with an estimated 350 000-400 000 customers in the Nordic countries. The greatest challenge is posed by well-established organized networks in Sweden, with upwards of 5000 customers a piece. To impede criminal investigation, the operators behind these networks have established large servers (web hotels) abroad. This trend is also noticeable in the other Nordic countries.

In the foreseeable future, substantial growth is expected in the areas of IPTV and streaming via Set-Top boxes (STB). Currently, investing in the conversion and delivery of high quality content is associated with high costs for illegal operators. The potential revenue loss for legal distributors of IPTV and streaming, is also quite substantial. Both in-house productions and the ability to procure television rights, are under threat.

In the coming years, Nordic Content Protection will be working towards increased safeguarding of digital rights through competence-building and collaboration in both national and international forums.

[1] The relevant technology is more thoroughly described in the chapter discussing technologies employed by criminals and in the attachments.

About Nordic Content Protection

Nordic Content Protection strives to prevent illegal access to television broadcasts received via satellite dish, digital terrestrial transmission, IPTV, cable transmission and streaming.

Nordic Content Protection is also currently collaborating with distributors to develop security solutions aimed at detecting and preventing illegal distribution.

Nordic Content Protection collaborates with the following Nordic distributors and rights owners: Com Hem Canal Digital, Boxer, RiksTV, Viasat, Telenor, Premier League, Divisionsforeningen, Onside, SBS Discovery, Norsk Fotball NFF, SHL, Norsk idrettsforbund og Olympiske og paralympiske komité, TV2 Norge, TV 2 Danmark, Cmore (TV4), FOX, Viacom, NagraVision.

More about these collaborations at www.stopnordic.com

About this trend report

This is the first trend report compiled for Nordic Content Protection. The report has several objectives. The first is to shed light on a relatively unknown form of criminal activity. The level of knowledge and proficiency in this discipline within law enforcement, prosecuting authorities and society in general, is relatively low.

The report also addresses the industry's expressed desire to take knowledge-based action, actively using the analysis as a foundation for future priorities, thus reaping the greatest benefits from the preventive and combative measures outlined.

This report deals with the Nordic market. Even though the methods and technologies employed remain the same, there are both national and regional differences in terms of application. This is especially true when it comes to operators and scope. Sweden stands out from the rest, with both more numerous and larger criminal networks. This is first and foremost a product of demographics combined with socioeconomic factors. Several Swedish court cases have resulted in numerous individuals being sentenced to pay seven-figure monetary compensation in addition to jail time.

Legislation and legal practices vary in the Nordic countries, as will be explained in brief in this report. More in-depth information can be found at www.stopnordic.com.

Methodology

The trend report is based chiefly on a qualitative method. It deals with a specialized discipline in which the expertise mainly resides with Nordic Content Protection. This has necessitated dialogue and a number of meetings with national representatives. Each one of these representatives has a network consisting of national players, business partners and sources inside the criminal networks. Additional sources of information include reviews of relevant court rulings, Internet searches and social media.

Current threats

The largest threat to the industry as a whole is the fact that *criminal networks challenge legal providers by offering low-priced illegal products with a wider range of services.* There are currently no legal providers able to offer a similar range of channels and services at the same prices as the criminal networks.

The industry consists of a multitude of competing providers of channels and broadcasts. Some of these have sizable overhead associated with in-house production, while others spend large amounts procuring the rights to content such as movies, TV-series and sporting events like the ever-popular Premier League. Subscribers pay a monthly fee or are billed on a pay-per-view basis for specific content.

The criminal networks offer an «all-in-one» solution in the form of a preconfigured STB. Customers can connect this device to their television sets and enjoy a wide variety of payed services on a single platform at a mere fraction of the cost of a legal subscription.

One extremely popular and widespread service is illegal «live streams». This service provides access to live transmissions of popular events, such as boxing matches and soccer games. This type of illegal service poses a growing threat to legal distributors and vendors. A large number of rebroadcasts are done from global servers, oftentimes free of charge to the consumer (ideologically motivated).

The criminal networks have become increasingly more professional over time. They are well versed with regards to international legislation governing audits and the exchange of information across national borders. A multitude of organized criminal networks have subsequently moved their servers to web hotels outside the Nordic countries, thus making it more difficult for national authorities to investigate them. There are currently precious few international entities

working in this field, a prime example being Europol, which is making no coherent effort to coordinate digital copyright breaches. This in turn provides fertile soil for increased criminal activity.

One example of the need for common legislation and international collaboration is found in Spain, where Nordic television broadcasts are sold to Nordic citizens who either reside in this country on a permanent basis, or own vacations homes there.

None of the Nordic distributors can legally offer this service, but there are currently several companies providing customers with illegal access to all Nordic programming through low-priced package deals that include a Set-Top box. The people behind these companies are Nordic citizens who have found a niche in the market. Taking legal action against them is extremely challenging as long as the servers remain on Spanish soil.

Financial loss – an estimate

Assigning an exact number to the financial damage currently being inflicted upon the industry by illegal operators in the Nordic countries, is no easy task. A modest estimate indicates an annual revenue loss somewhere in the neighborhood of 4 billion NOK.

Nordic Content Protection estimates that in Sweden alone, there are around 250 000 households connected to illegal networks. Add roughly 50 000 households per country in Denmark, Finland and Norway, and the Nordic tally rises to an estimated 400 000 illegal users. These are reasonably realistic figures based on reliable sources and experience, as well as criminal court cases, both past and present.

The price of a basic program package tied to a legal subscription is around 300 NOK per month. Premium channels will run subscribers an additional 200 to 400 NOK in monthly fees. An illegal provider will, on the other hand, offer customers access to every channel on the market without any additional fees. With around 400 000 customers buying illegal services, the annual revenue loss for the legitimate distributors adds up to roughly 4 billion NOK.

Exactly how much money the criminal operators are taking in, is unknown. There are numerous criminal networks active in the market, with varying services and price structures. A fairly normal price for subscribing to illegal channels and services is around 1500 NOK per year. 400 000 customers results in an annual turnover of approximately 600 million NOK.

An example of current legal practice is a sentence passed in October of 2015 in Södertörn Tingsrätt (B-8110-11) in Sweden. Two individuals from a criminal network were convicted of cheating Canal Digital, Viasat and Com Hem by offering customers illegal access to their TV-packages, with content from 27 payed television providers. The network was active from

September 9, 2010 to June 9, 2011, at which time it was servicing 1150 customers. The plaintiff companies where awarded more the 8,1 million SEK in damages.

Where does the illegal money go?

Nordic Content Protection has over a period of years documented how illegal operators have spent large amounts of money on personal consumption, exclusive cars and luxury items. There has, however, been a change in recent years. Ongoing investigations have revealed a new trend in which illegal proceeds are transferred to foreign accounts in conflict areas.

Investigations have also revealed that criminal operators are investing large sums of money in real estate and legitimate companies, both in and outside of the Nordic countries. Some operators are also active in other criminal fields, and they reinvest their proceeds in the illegal economy.

Who purchases illegal services and how?

The people who buy illegal services from criminal networks, come from nearly every demographic and walk of life. The shear diversity of this group makes the task of launching a targeted effort to deter current and potential customers extremely difficult. There are, however, certain geographical areas that statistically have lower number of legal subscribers than one would expect in comparison to the rest of the country. This could be an indicator of the existence of illegal networks in the aforementioned areas.

Signing up for these illegal services can be done in several ways. The user «NOMORE» aptly sums up the illegal market on the website diskusjon.no (a site for people interested in technology):

> *"You don't seek out large CardSharing networks who market themselves. You find a network in your local community and enquire about membership in a very hush hush manner. In this way the networks remain small, since nearly all of the members know each other, and there's little risk of being caught.*
>
> *Networks actively marketing themselves obtain more customers, but the resulting attention boost increases the risk of being caught. This applies to both operators and customers. The downfall of these networks is typically greed.*
>
> *Who do you think the authorities and legal distributors are going to focus their efforts on hunting down? The hundreds of smaller networks with 20-30 members, or the big ones with hundreds, sometimes thousands of members, of which there are relatively few? "*

Technologies employed by the illegal networks

These are the current threats, ranked in prioritized order in terms of scope and prevalence:

1. Cardsharing
2. IPTV
3. Streaming

Cardsharing networks remain the biggest threat to the industry in terms of prevalence and financial damage. However, IPTV is expected to overtake cardsharing as the number one threat within a few years. This will happen as soon as the necessary technical equipment becomes an affordable investment for the smaller criminal networks. Additional contributing factors are technology impeding illegal distribution through encryption and other security solutions.

An additional description and illustration of the various technological methods is found in the attachment.

Cardsharing

Cardsharing is when several people share one of more TV-cards over the Internet in a cardsharing network. The network consists of several interconnected cardsharing servers distributing television content and a number of cardsharing clients receiving television signals. In terms of practical application, only the control codes are being shared in this network – not the actual television broadcasts. They are decrypted and forwarded via a server to the customer when he or she selects a TV-channel.

Streaming

Streaming via websites is when audio and video is braodcast over a computer network in a way that allows the end user to enjoy the content in realtime without having to wait for the entire file to download. Each bit of content is readily comsumable as soon as it reaches the client. Simply put, this means that you can go to a website and watch TV-series, movies, entertainment programs and live broadcasts. The stream becomes illegal when one distributes broadcasts that other parties have bought the exclusive rights to show to their viewership. In addition to being a legal offense, breaching these rights can result in substantial revenue loss for the rights owners. Putting a stop to streaming is a monumental task, as illegal operators and servers are found all over the world.

IPTV

IPTV via hardware, is an abbreviation for Internet Protocol Television. Transmissions are digital and usually require the use of the provider's decoder.

Operators offering IPTV illegally, do so under the guise of being legitimate enterprises. They often offer package deals – i.e. a decoder and a subscription with a broad variety of channels, including films and sports (Nordic channels) – at prices way below the going market rates.

The current trend is an increasing number of criminal networks offering illegal IPTV in the Nordic countries.

Criminal networks – three ideal types

The active networks in this particular crime sphere bear similarities to networks operating in other areas of financial and organized crime with regards to operators, scope, logistics, size and economics. Some organized criminal networks have made a profitable transition from more serious avenues of illegal activity. This type of crime carries a lower penalty, and a relatively modest investment can result in a massive profit.

The common denominator for these networks (except for ideological and political ones) is that payment is usually done in cash. Some have, however, opened accounts to enable payment through bank transfers and postal money orders. For logistical reasons, the cash transactions are usually done on a quarterly, biannual or annual basis. Payment is either collected by the vendor, or delivered by the customer at a designated drop-off point, like a mailbox. All networks keep ledgers containing customer lists, payments et al. The subscription period usually coincides with payment frequency, the most common being three or six months.

Buddy networks

These networks are very common. They are typically established by individuals who belong to the same group of friends, often in the same geographical region. Very few of these people have prior convictions or ties to known criminal gangs and networks. These are simply cardsharing networks driven by the desire to save money. Taking part in a cardsharing network saves the individual members a lot of money when compared to buying the same services at normal prices. Experience has shown that these networks are hard to uncover.

Ideological and political networks

As their names imply, these networks are run by individuals who are either ideologically or politically motivated. Many of these individuals are active members of networks involved in piracy and hacking on closed forums. They possess a high degree of technological proficiency and offer other forum members free cardsharing and IPTV.

The main threat posed by these networks is their ability to detect weaknesses in the industry's security solutions - which in turn may be exploited by other illegal operators in their own criminal pursuits.

Organized criminal networks

These networks are run very much like a legitimate business. They have a clear and defined structure, with designated personnel in charge of sales, finances and technology. They have access to individuals who possess an abundance of technological know-how, and they have high capacity servers in web hotels, which in most cases are located abroad.

Some of the larger networks operate behind a legitimate façade, quite often a retail store selling decoder devices and other related merchandise. Other networks are clandestine operations, where contact takes place solely via other customers. These networks are highly profitable. Some of them have upwards of 5000 customers tied to their cardsharing networks. Some of the networks uncovered so far had made millions before they were terminated.

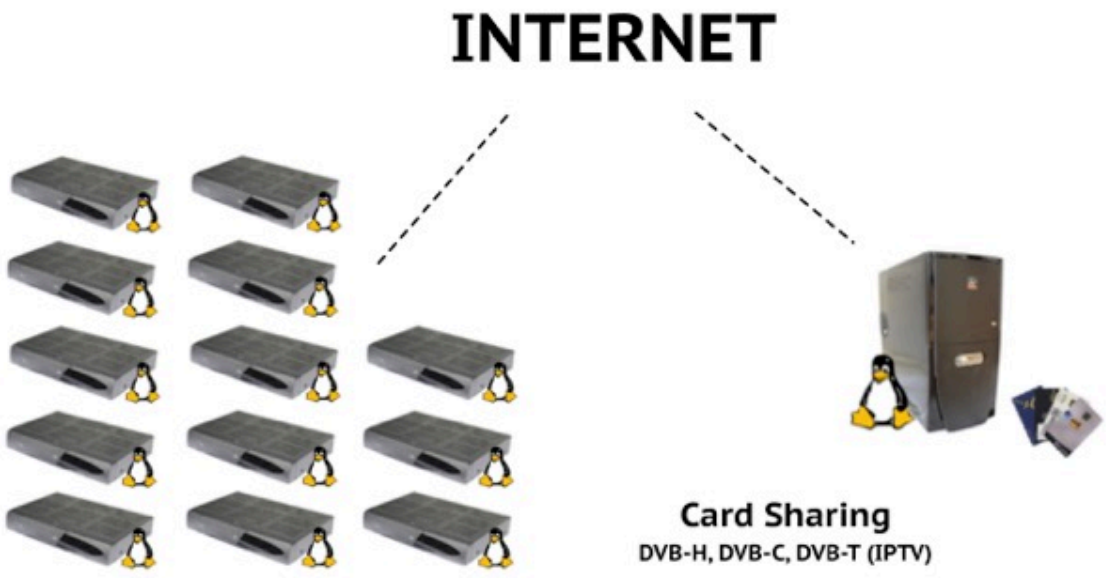
Many of the people associated with these organized networks are also involved in other criminal endeavors and are affiliated with other criminal networks. It is therefore a reasonable assumption that part of the illegal proceeds are used to finance other criminal activities - the worst case scenario being terror.

Recommendations

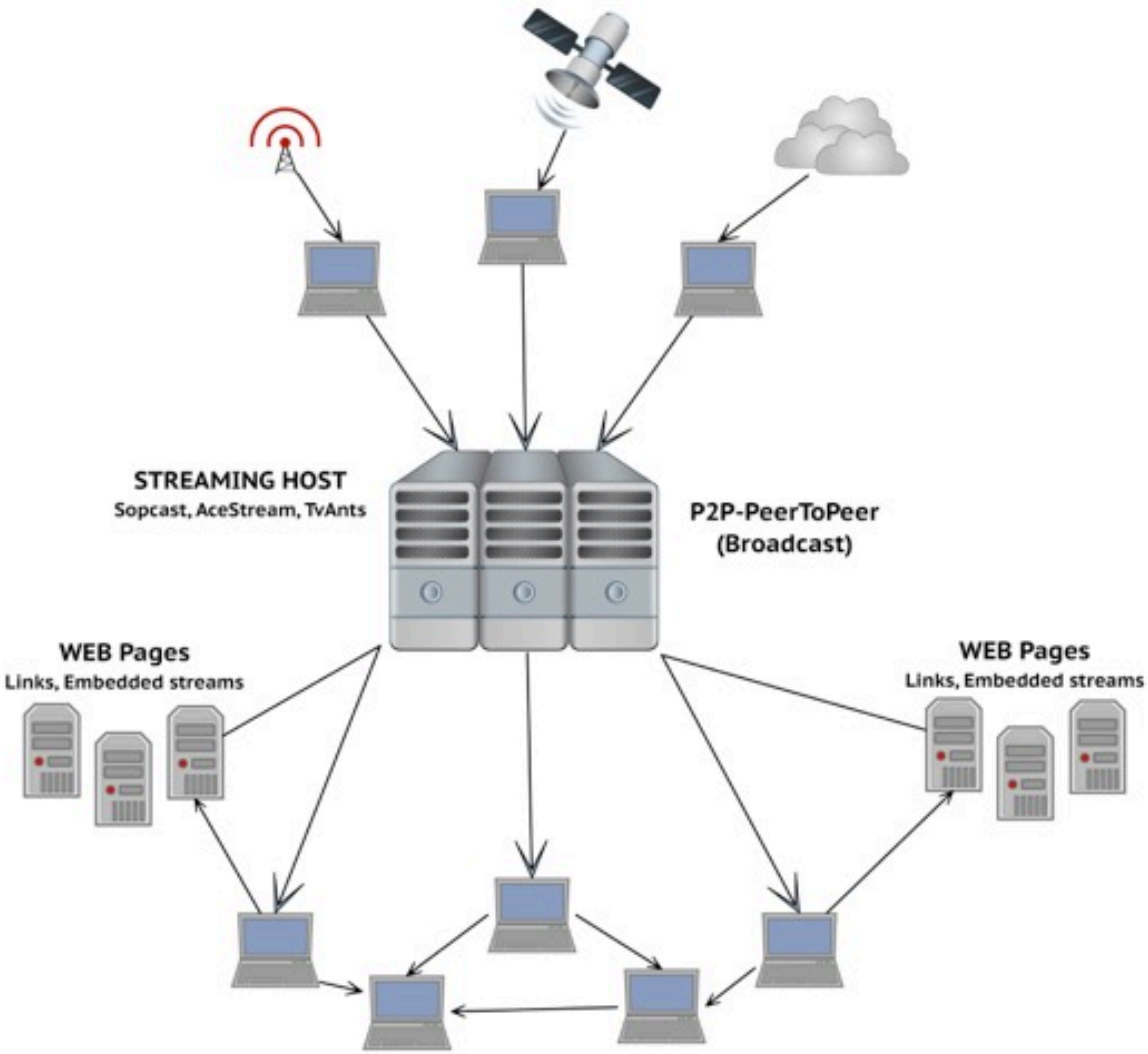
In order to combat and ultimately prevent the activity of illegal networks and ensure the livelihood of legitimate players in the industry, the following measures are recommended:

1. *International police collaboration led by Europol to protect transnational digital copyright.*
2. *Increased competence building amongst national and international business partners.*
3. *Establishing IPR-units in all Nordic countries. Finland and Norway presently have no such units.*
4. *Technical solutions to increase security on the respective platforms.*
5. *Finding a functional solution regarding illegal content from abroad.*
6. *A change in practice to legally limit access to these illegal services. Ideally, a petition from the prosecuting authorities should be enough to have these services filtered.*

Attachment 1: Illustration of a cardsharing network



Attachment 2: Illustration of streaming via websites



Attachment 3: Illustration of an IPTV-network (streaming via hardware)