



N O R D I C
C O N T E N T
P R O T E C T I O N

Annual Report 2019

- Data, patterns and statistics -

Executive summary

Nordic Content Protection publishes annual reports to share knowledge and data in an effort to raise awareness about the scope of TV-related violations of intellectual property rights.

This Annual Report 2019 centers on the data we collect, when gathering intelligence from online open sources. Our investigations are all intelligence led, allowing us to base important case-related decisions and prioritizations on the basis of concrete information. In a time where everyone can become an illegal TV provider in a matter of minutes, and where organized criminal groups are also entering this particular lucrative field of crime, this is, from our perspective, the optimal way to remain agile and prepared when working with enforcement of television rights.

The statistics presented in this report reveal that while card-sharing servers are still active and a key component for the illegal TV signal transcoding, the numbers of servers are significantly decreasing and have been for the past three years. Nearly 80% of the identified card-sharing servers are located in either EU or the US.

As a result of effective enforcement over a prolonged period, card-sharing servers in the Nordic countries represent 4,5% of the global count and of those more than 50% are hosted in Sweden. The use of Nordic Internet service providers for hosting card-sharing servers has proven to conform to the largest Internet service providers in each country. In one instance though, we are able to detect a high number of card-sharing servers making use of a hosting provider with notable lesser market cap, thereby indicating that the hosting provider is preferred by the illegal actors.

Providers of illegal IPTV are rapidly increasing in numbers. This is well represented by the growing number of new websites being launched as points of sale. The NCP Blacklist was created to consist of websites selling illegal IPTV and have seen an increase of 274% since 2016. Of all websites added to the list in 2018, more than 70% was detected within 10 days after the registration of the used domain names. With this effective level of detection and with proper procedures in place, the NCP Blacklist is a critical indicator of the threat level posed by the illegal IPTV providers.

New illegal IPTV websites are mainly launched during European winter months and 77% of the NCP Blacklist websites has implemented 'IPTV' in the domain name. More than 60% of the illegal IPTV websites use .com as their top-level-domain. Only 1% make use of Nordic country code top-level-domains. Regarding hosting, the pattern is aligned with that for card-sharing servers in that very few illegal IPTV websites are using Nordic hosting providers.

Table of contents

Executive summary	2
Table of contents	3
Introduction	4
About this report	5
About Nordic Content Protection	5
Data, patterns and statistics	7
Card-Sharing	7
Number of card-sharing servers	8
Location of card-sharing servers	9
Nordic card-sharing servers	11
Card-sharing hosting providers	13
Nordic card-sharing hosting providers	13
Card-sharing hosts preferred by illegal actors	16
IPTV	17
Illegal IPTV monitoring	18
NCP IPTV Blacklist	18
IPTV website domain names and registration	19
IPTV website hosting	22
List of figures:	24

Introduction

Welcome to the fourth annual report by Nordic Content Protection (NCP). Our previous annual reports from 2016 and 2017 highlighted current trends and developments regarding threats against the TV industry. Last year we used the report to provide insights into the operational reality of intellectual property rights enforcement.

This year our annual report focuses on two current major threats facing the television industry, namely card-sharing and illegal IPTV. NCP is continuously working against these threats on several levels, and a vital part of this work is monitoring and analyzing them.

To monitor a multilayered and very resistant threat landscape, NCP have developed and used a range of effective and proven methods of collecting data from open sources. Data which, when analyzed, enables us to prioritize and target the most acute threats. These are often organized criminal groups earning substantial profit from major TV rights violations. An example of such a group can be found in the Swedish Patent and Market Court ruling against ATN (Advanced TV Network AB) in July 2018¹, in which the defendants was sentenced to prison and ordered to pay more than €20 million in damages to two main TV right-holders. A case which was investigated and reported to authorities by NCP in 2016.

With this report, it is our ambition to showcase and visualize a lot of the data we collect. In the name of knowledge sharing, we welcome any reader to contact us for a discussion or for further elaboration.



¹ Reuters. [Arabic internet TV firm fined \\$24 million for sports rights piracy](#)

About this report

As this report is about data patterns and statistics, there will be little focus on the operational measures employed by NCP. To read more about these measures, we encourage you to read the NCP Annual Report from 2018, in which we described two relevant case studies.

Certain metrics as well as website domain names are not included in this report. These omissions are done for confidentiality and data privacy.

When the terms Nordic or Nordics are used in this report, they cover the countries Denmark, Finland, Norway and Sweden.

About Nordic Content Protection

NCP is a not-for-profit member association dedicated exclusively to intellectual property rights enforcement for the television industry. With more than 18 years of practical experience and numerous impactful results, NCP continues to prevent illegal access to television content received via satellite, digital or terrestrial transmissions as well as illegal IPTV and general streaming via the Internet.

Our team consists of technicians combined with experienced high-tech crime investigators from Nordic and international police forces. This particular composition of specialists allows us to remain agile and adapt our efforts to the continuously changing threat landscape. We cooperate closely with NCP members and carry out numerous enforcement actions ranging from content take-down to large scale multinational investigations.

NCP believe in sharing knowledge as well as data, when it supports our and our members' agenda in combating the overwhelming magnitude of IP infringements targeted at the TV industry. In achieving this we prioritize working with multiple international partners such as Europol, EUIPO and other EU institutions in addition to national police forces. To these partners we offer training and case support on an ad-hoc level.

To learn more about our work and results, visit our website at www.ncprotection.com. Find an overview of current NCP members below:



Data, patterns and statistics

Collecting data from open sources is a key component in our intelligence gathering. It is essential to be able to quantify and monitor developments in the overall threat landscape. Without a high level of intelligence, it is not possible to fully understand the illegal activities and therefore not the scope of violations they represent. In addition, to counter experienced, skilled and financially motivated criminals, who often benefit from new and emerging technologies, you need as much intelligence as possible.

Collected data, if stored and handled correctly, can also be utilized as evidence in later cases. In fact, structuring and analyzing the data is very often the foundation on which NCP decides which cases to investigate further and forward to authorities.

The following sections will focus on data, collected by NCP for two of the main threats to the TV industry at this point in time - card-sharing and IPTV.

Card-Sharing

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

NCP have been identifying card-sharing servers on the Internet for a range of years. We mainly focus on establishing which are illegal servers within the Nordic region, i.e. hosting, Nordic channels or other relations to our Nordic members.

In regards to how many active card-sharing servers we have identified and monitored, we will, in this report, look at data collected since 2015.

Number of card-sharing servers

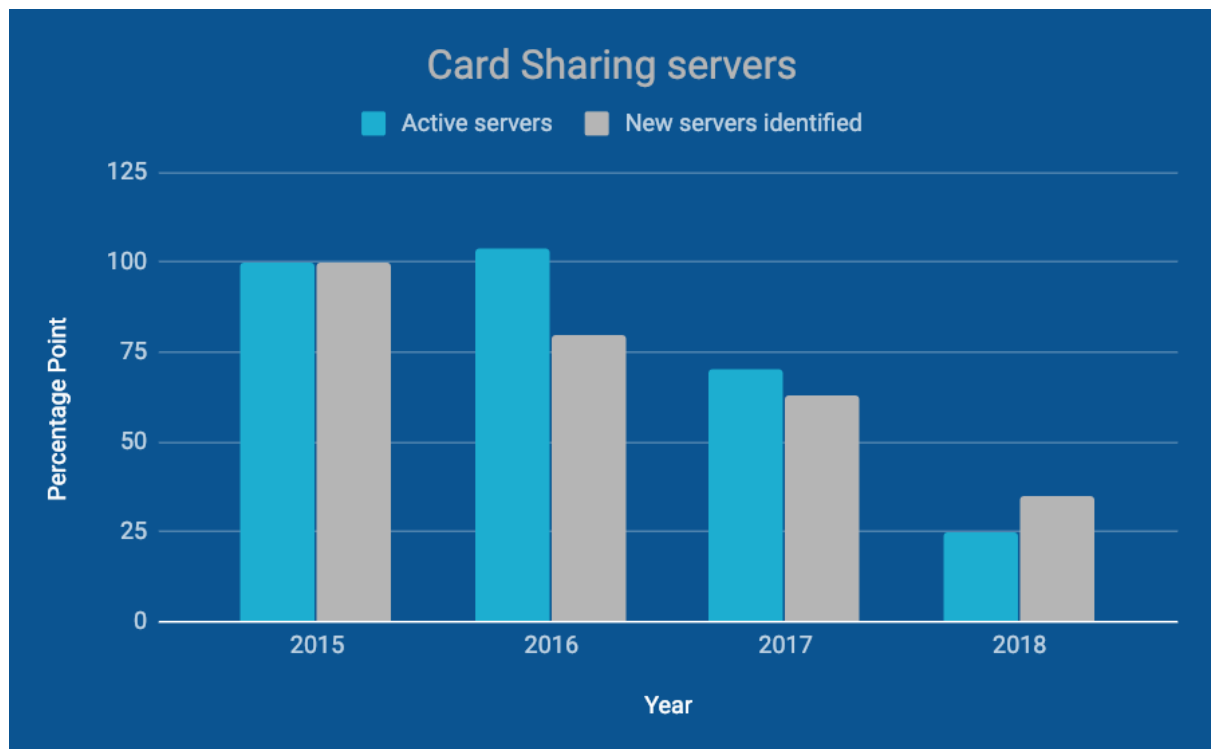


Fig. 1.

From Fig. 1 it is clear that the overall number of card-sharing servers (blue columns) is declining. We observed a small increase in the total number of identified active servers in 2016, but for the following years we have seen a significant decrease. By the end of 2018 the number of active card-sharing servers is down by 75 percentage points compared to 2015.

The described decline is supported by data, gathered in the same period, regarding the numbers of new card-sharing servers identified (grey columns). New detected server numbers show a steady decline per year to a total of 65 percentage points from 2015 to the end of 2018.

It is likely a combination of different reasons resulting in the substantial decrease in the number of card-sharing servers. A few main reasons are:

- In 2014 Swedish legislation was updated, which meant that it became illegal to be customers of card-sharing networks. The effect of this was immediately evident in 2015, when the first conviction of a customer took place. Similar legislation was already in place in the other Nordic countries.
- NCP, NCP members and other stakeholders have unceasingly pushed back against card-sharing networks. By identifying the criminals and reporting them to authorities, we have contributed to numerous successful cases, and

subsequent card-sharing server removals. Many of these cases have received media coverage, which also, proactively, work against the illegal networks.

- The technological developments. Mainly access to affordable high speed Internet capacity and server rental, resulting in new alternative business models such as IPTV. But also deployment of technical countermeasures by right-holders. In combination, this is to a large extent the reason for the current observable migration from one illegal platform - card-sharing - to another - IPTV.

Location of card-sharing servers

Every identified card-sharing server reveals a geographic location. This allows NCP to identify patterns regarding where it is hosted. For several years we have been able to observe a large drop in the number of active servers being hosted in the Nordic countries. The reason for this development is analogue to the reasons listed above for the general drop in numbers. But another explicit reason here is the enforcement activities carried out by NCP and NCP members, in cooperation with Nordic national authorities. These enforcement activities have effectively removed the illegal servers from Nordic countries. To achieve results like this, established and effective procedures has to be in place as they are in the Nordics. Then immediate intervention and action is possible, when the relevant intermediary (i.e. hosting companies) are compliant to national laws and based in a Nordic country.

However, illegal actors in the Nordics are aware of the mentioned procedures and potential consequences. And as a result they mostly place their illegal servers in countries outside Nordic jurisdiction². Unfortunately this has little negative impact on the illegal activities, as administration of these can be carried out remotely without problems. On the other hand, it generates substantial challenges enforcement-wise, as international collaboration between authorities handling IP crimes continues to be slow and ineffective, often resulting in investigations being unnecessarily prolonged.

² Europol. [2017 Situation Report on Counterfeiting and Piracy in the European Union](#) p. 29.

Between 2015 and 2018 these are the top ten hosting countries:

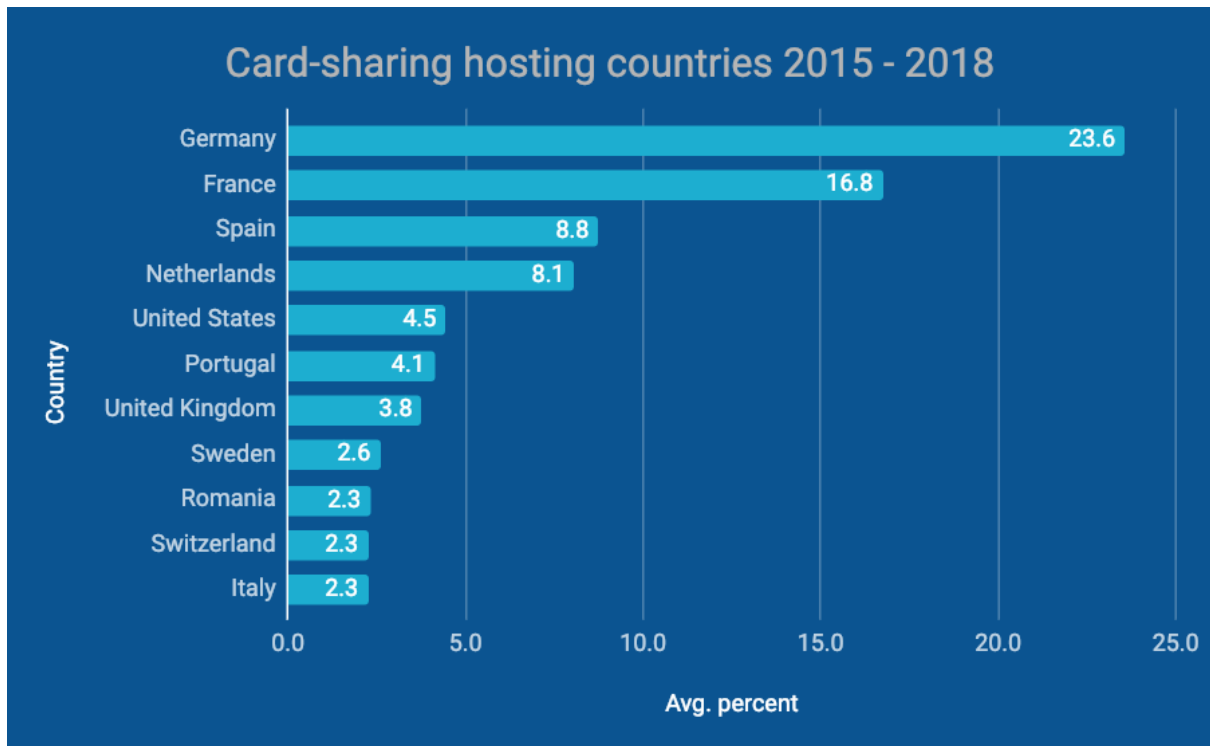


Fig. 2.

Or as shown on a world heatmap:

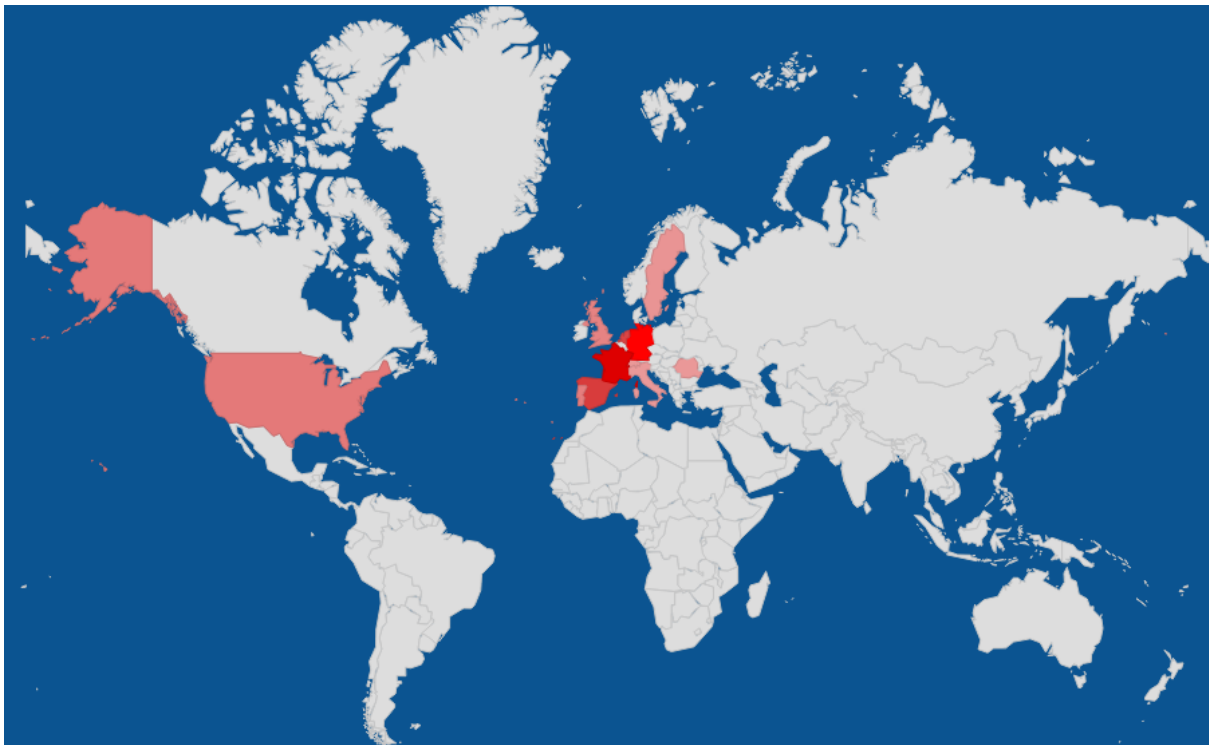


Fig. 3.

From Fig. 2 we are able to see that on average Germany has been the country of hosting for more than 23% of the active card-sharing servers between 2015 and 2018. Fig. 2 and Fig. 3 also show, that apart from United States, all top ten hosting countries are located in Europe. Regarding Nordic countries, only Sweden is part of the top ten list, with an average of 2.6% of the illegal servers for the period.

Use of European based hosting companies is a well-known pattern within illegal TV activities. The main reasons for this is the highly developed Internet infrastructure, allowing for stable high speeds and crucial network traffic capacity, as well as a current competitive European market of hosting providers, resulting in very affordable prices.

Despite the mentioned challenges surrounding international cooperation between authorities, the fact that the majority of all active card-sharing servers are hosted in Europe or the US, speak in favor for continuous future enforcement actions.

Nordic card-sharing servers

When comparing the numbers of active card-sharing servers in the Nordics against the total number of servers, we learn that they collectively represent 4.5%. Fig. 4 below shows the share of servers for the Nordic countries.

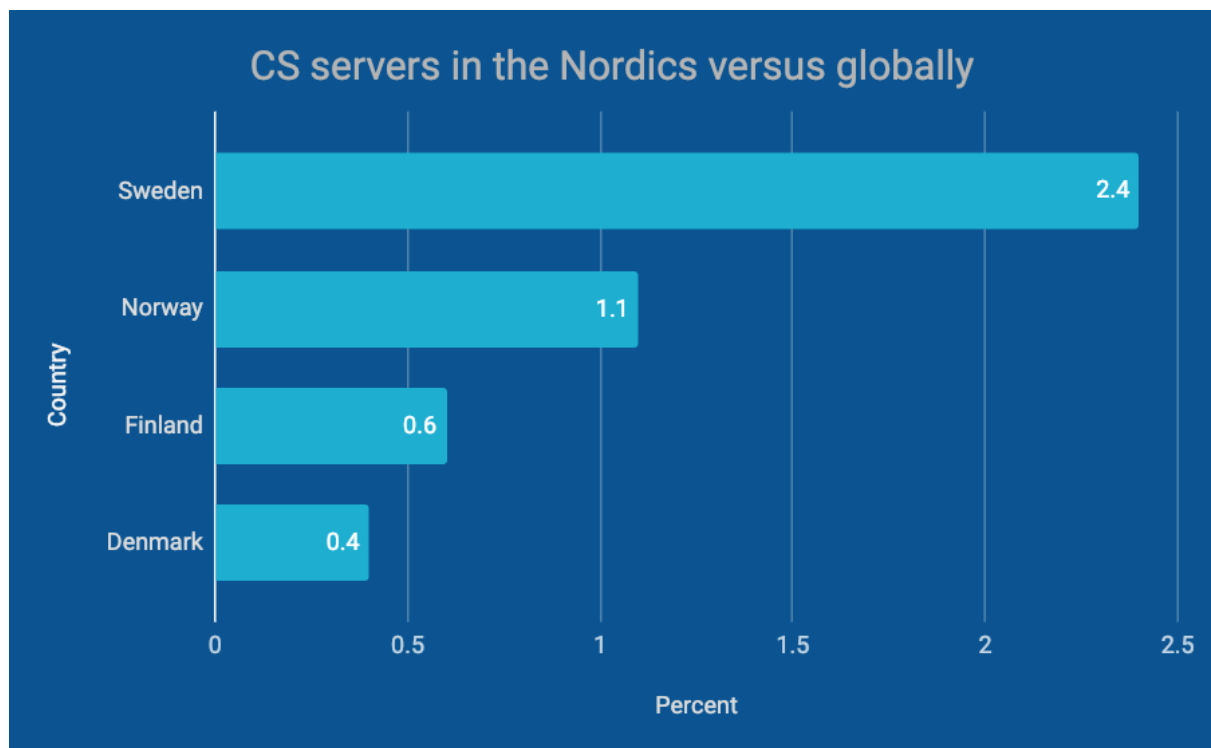


Fig. 4.

The distribution of active card-sharing servers within the Nordics shows that Sweden with 52,2% holds the highest percentage. See Fig. 5 below.

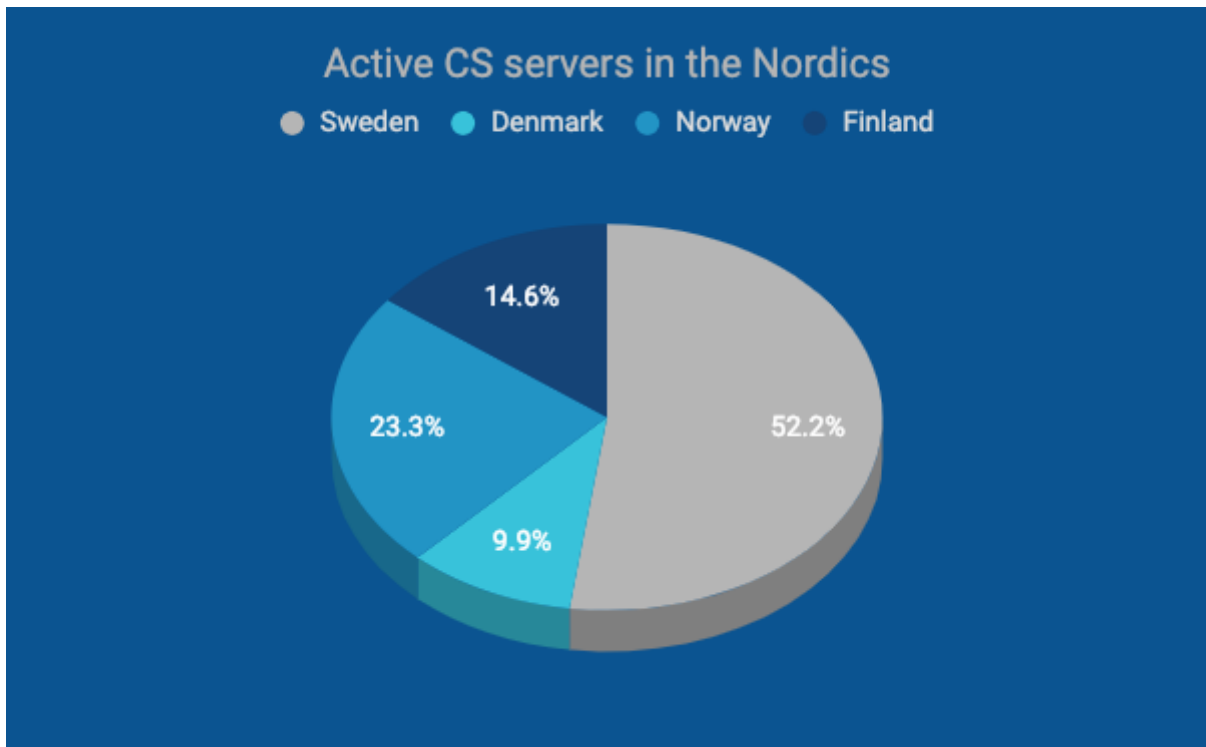


Fig. 5.



Card-sharing hosting providers

Finally, when monitoring server locations, we are able to observe which hosting providers are being utilized by the illegal actors. By analyzing data for the 2015-2018 period, it is obvious that a large number of different hosting providers has been used. Below, in Fig. 6 is the top five most used hosting providers for the mentioned time period.

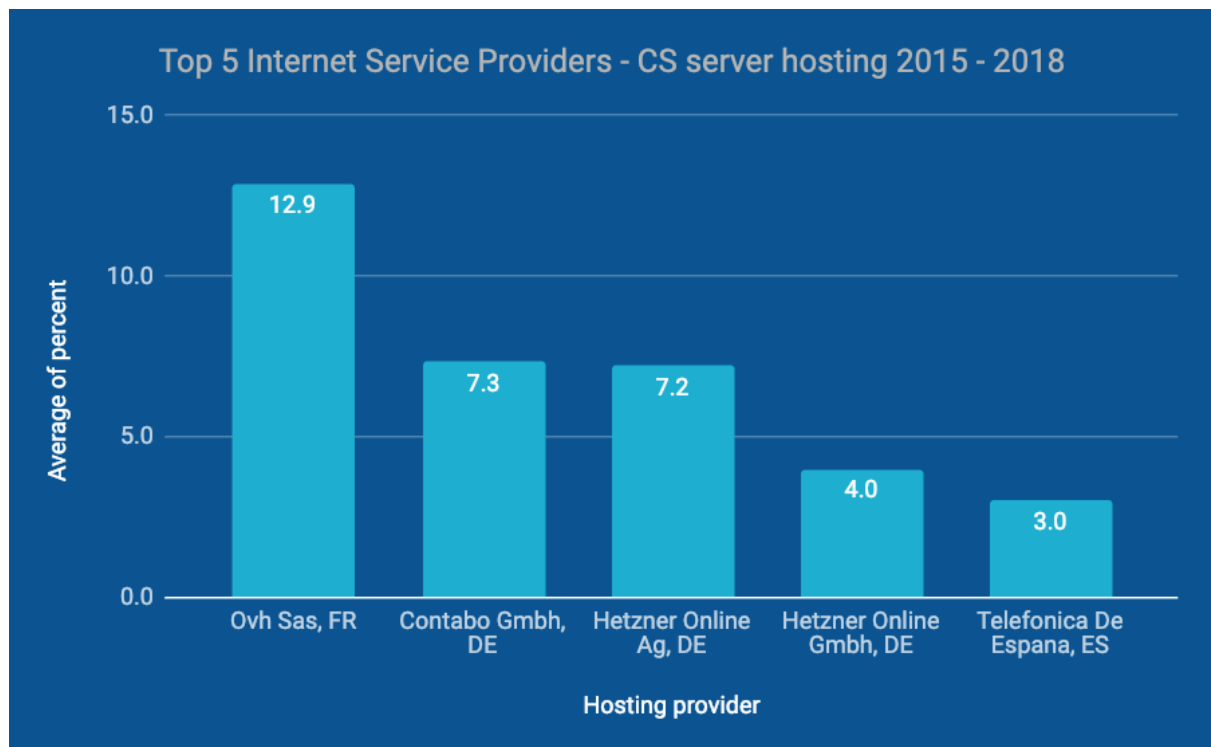


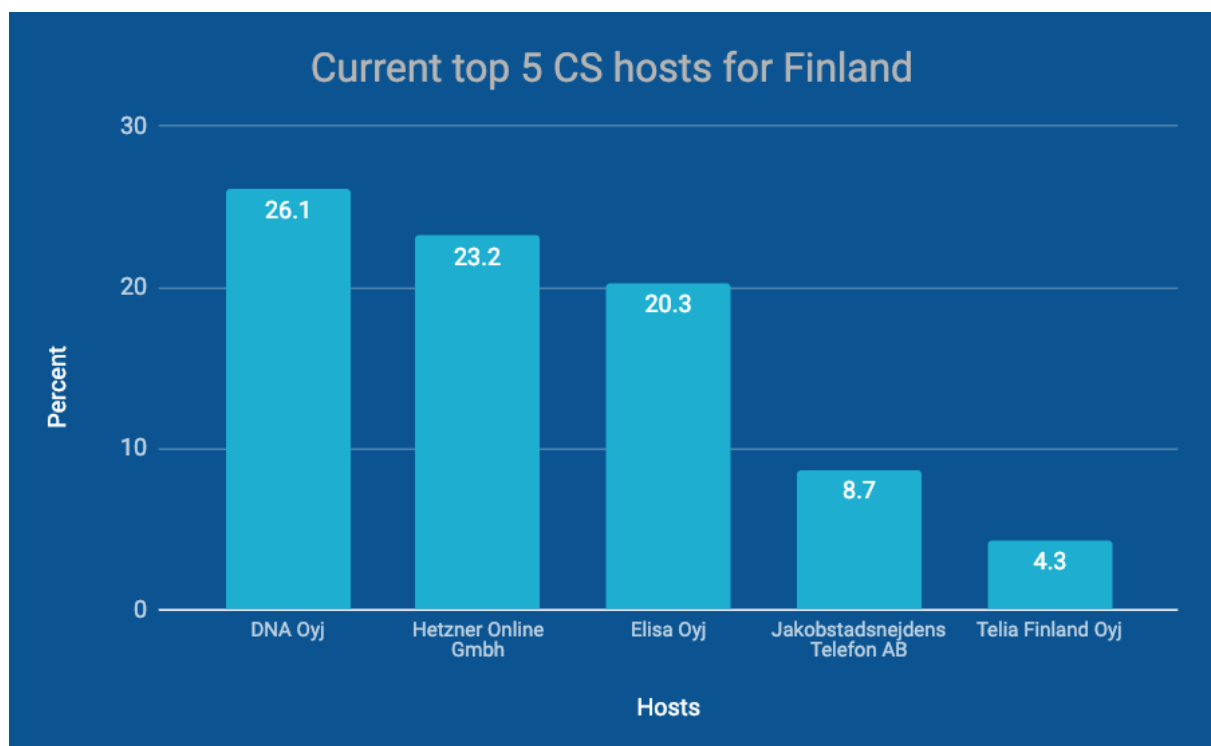
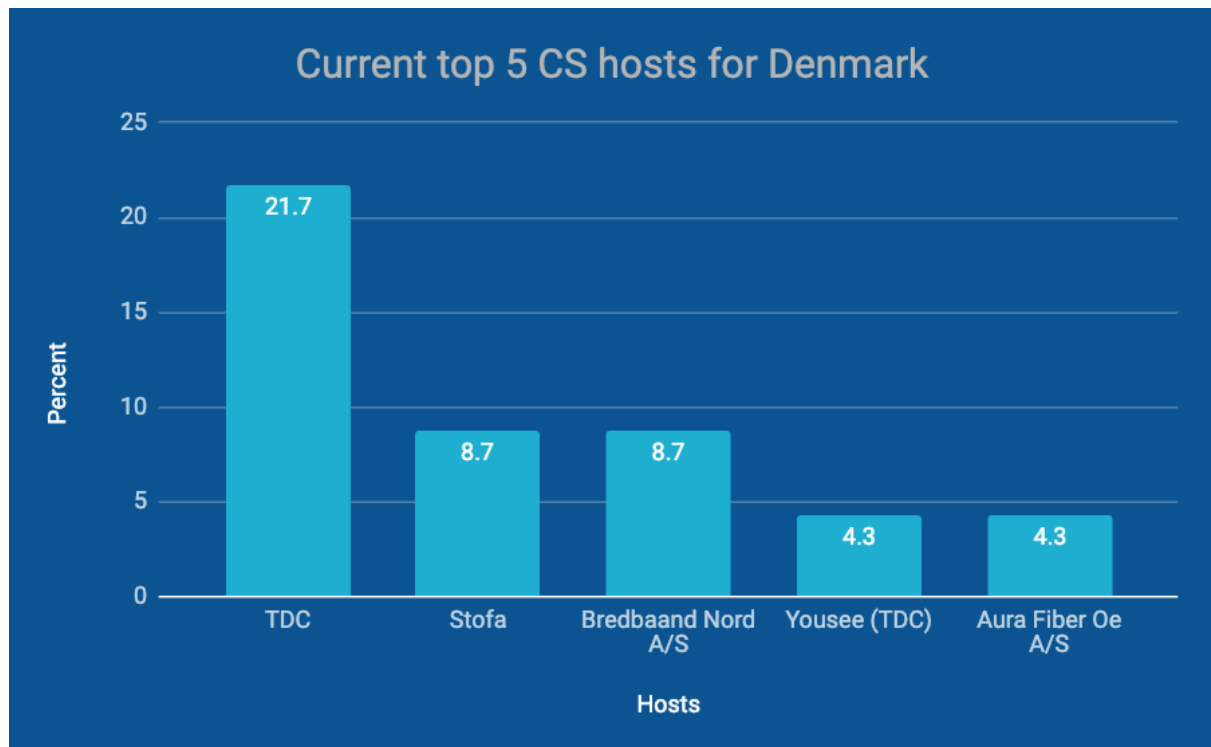
Fig. 6.

As anticipated, based on what we learned from figure 2, German, French and Spanish hosting providers dominate the top five. No Nordic based hosting providers makes it into the top five or even top ten.

Nordic card-sharing hosting providers

Hosting for card-sharing servers obviously also takes place in the Nordics. For years NCP have used identified hosting data connected to Nordic hosting providers, when reporting cases to authorities.

Experience shows that card-sharing server operators very often run the servers from their homes, using their private Internet connections. On this basis, we should theoretically see the largest national Internet access providers represented among the most frequently used Nordic hosting providers.



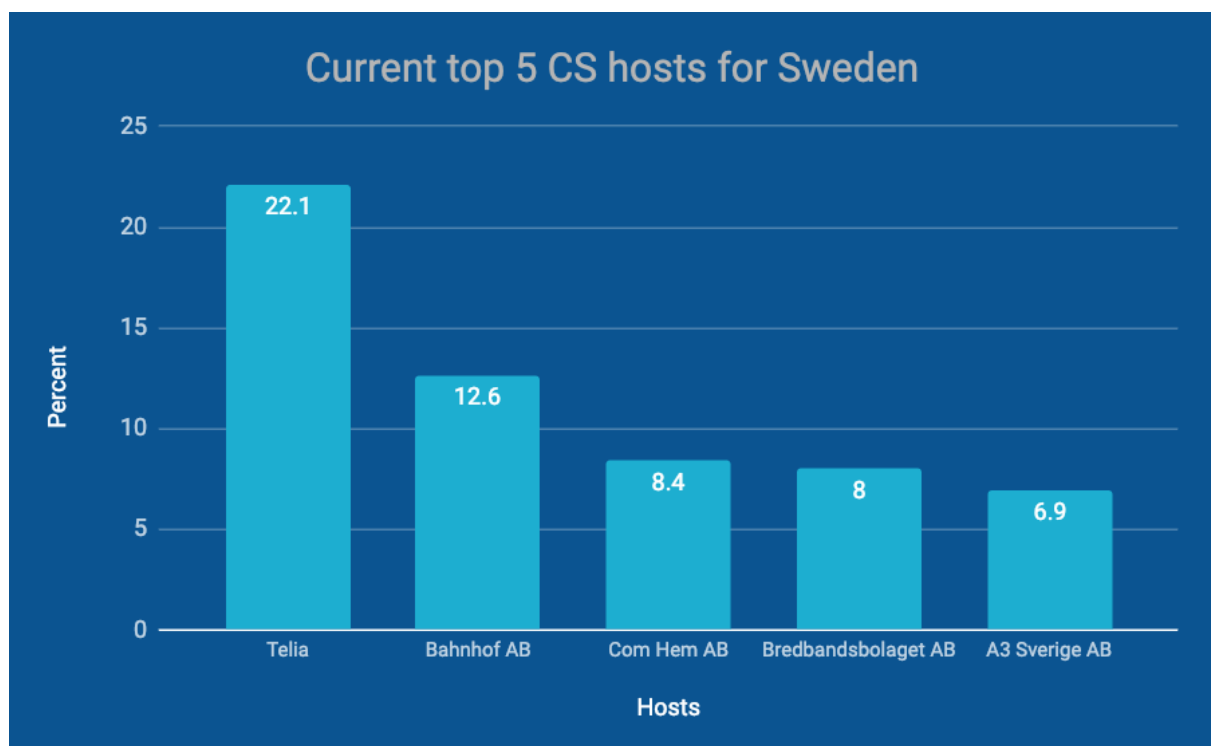
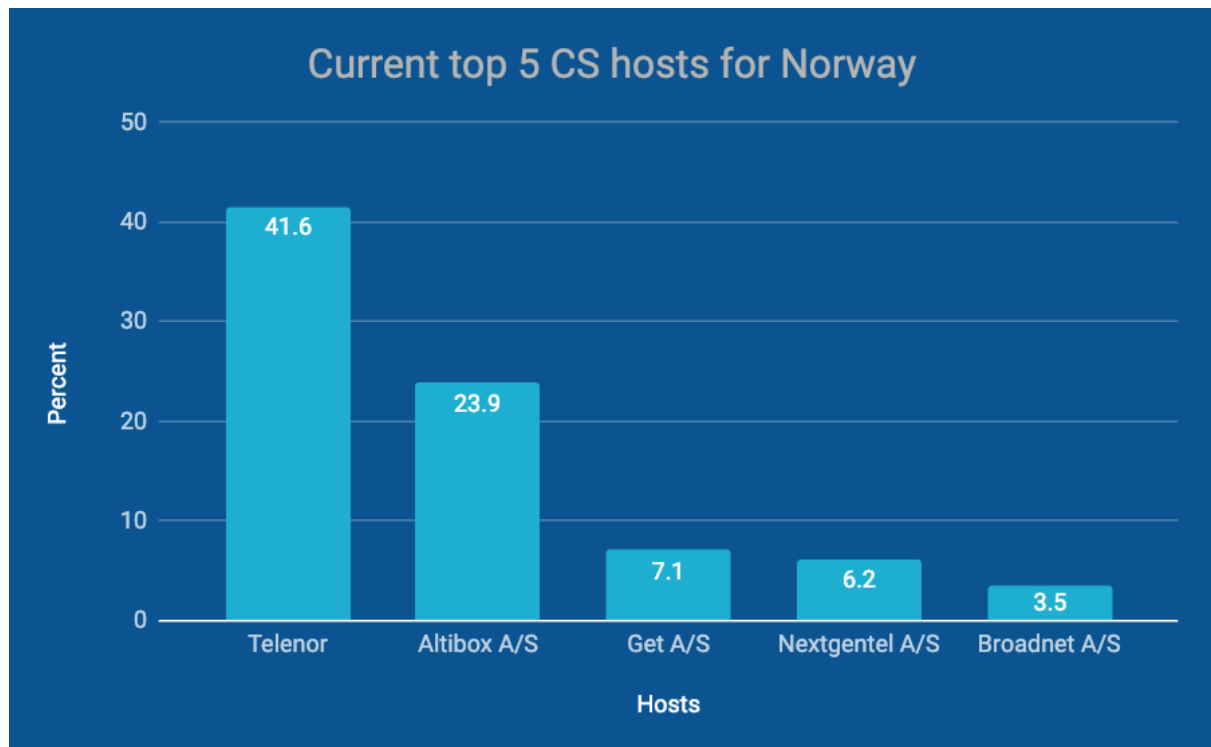


Fig. 7.

Overall, data in Fig. 7 confirms that, for the Nordics, the large Internet access providers in each country are also, to a large extent, the most exposed to have their infrastructure used by Internet access customers running illegal card-sharing servers.

Card-sharing hosts preferred by illegal actors

Intelligence gathered by NCP, from different communities related to illegal TV activities, reveal that both illegal TV providers and users/customers share information about how to best acquire and maintain well functioning illegal pay TV access. One topic that receives a lot of attention in online forums is which Internet access providers to choose. This is relevant as both server admins as well as customers wish to avoid restrictions such as closed network ports and unstable connections. These discussions also consider, which Internet access providers are more or less likely to comply to requests by law enforcement or authorities in general, and in that regard, which data might be stored about customers.

By observing these frequent discussions, NCP believe that, to some extent, illegal TV providers/customers are likely to choose certain Internet access providers over others.

NOTE: Before giving the following example, NCP wish to emphasise that none of the mentioned Internet access providers are knowingly supporting the operation or use of the identified card-sharing servers.

With the data for Sweden presented in Fig. 7 above, we are able to see, that the most frequently used host for card-sharing servers in 2018 was Telia, accounting for 22.1%. This correlates well with the fact that Telia was the largest Internet access provider in Sweden with a market share in 2017 of 33.5%³.

For Internet access provider Bahnhof AB, with a market share of 6.7%, but hosting 12.6% of the card-sharing servers in Sweden, we notice a pattern, which indicate, that communities within card-sharing operators appears to prefer this Internet access provider to others.

³ <http://www.statistik.pts.se/media/1315/svensk-telekommarknad-2017.pdf> p. 34.

IPTV

Illegal IPTV is use of the Internet Protocol to digitally broadcast television, without obtaining the appropriate legal rights to the content. It is available on all popular devices such computers, tablets, smart phones, smart TVs and via set top boxes. For a range of years the number of illegal IPTV providers have been increasing at a rapid pace^{4 5} and today it constitutes one of the most significant risks to the overall TV industry.

Illegal IPTV is generally sold as subscriptions via dedicated websites or via social media (mainly Facebook and Skype). Additionally, experience shows, that illegal IPTV also continues to be sold in the physical world, from street shops and through personal networks.

The illegal IPTV providers/vendors can generally be divided into two categories:

- Large scale providers, who facilitate transcoding of encrypted satellite TV signals into digital streams to be included in the offered IPTV subscriptions. These providers trade/exchange the transcoded signals (channels) with other large scale providers. Furthermore, these providers support large number of customers and often have highly developed reseller plans, which allow them to generate additional “passive” profit. Large scale providers frequently sell preconfigured set top boxes in addition to online IPTV subscriptions.
- Resellers, who sign up with one or more large scale providers and resell either online IPTV subscriptions or combine them with set top boxes. Resellers usually pay a “signon” fee as well as commission or fixed rate per customer they sign on.

It is not uncommon for both types of illegal IPTV vendors to offer IPTV subscriptions containing several thousand TV channels, as well as equal numbers video-on-demand titles.

A main barrier faced by illegal IPTV providers is the increasing demand on network infrastructure. Specifically, a high total number of concurrent viewers demands for high level network bandwidth. This necessity for increasingly high bandwidth is a key reason, why most identified IPTV streaming servers remain located within Europe or the US, where Internet infrastructure highly developed. In certain cases, we have learned that some IPTV providers also chose to provide hosting services and other related services, essentially making them regular Internet service providers.

⁴ Europol. [2017 Situation Report on Counterfeiting and Piracy in the European Union](#) p. 29.

⁵ UKIPO. [IP Crime and Enforcement report 2017/18](#) p. 30-31.

Illegal IPTV monitoring

NCP has been monitoring individual websites and social media profiles used to sell illegal IPTV for a number of years. As a result, we are able to monitor developments in volume as well as form and content.

One main development in illegal IPTV, observed during 2017 and 2018, is how effortless it has become for nearly anyone to become an illegal IPTV reseller. Made possible by a number of large illegal IPTV providers, who have created a business model around providing an easy to use infrastructure, where aspiring resellers can sign up, pay an often required reseller fee and configure and prepare the system for customers. With this development, a person can become an active reseller of illegal IPTV within only a few minutes. Many new resellers select a dedicated website as their primary point of sale. Inexpensive domain name registration and website hosting as well as e-commerce software also contribute to the overall increase in the number of illegal IPTV providers.

NCP IPTV Blacklist

To monitor the IPTV threat landscape, NCP use automated detection and threat scoring in combination with manual verification. The algorithms used to carry out this work primarily work to detect websites selling illegal IPTV with a Nordic impact. Meaning for example that the website sells IPTV subscriptions with Nordic content, or that the website is specifically targeting Nordic customers.

The result of this work is the NCP Blacklist containing websites selling illegal IPTV. The list is divided into different categories and numerous details concerning each website are collected. As an example we are able to know that 60% of the websites in the NCP Blacklist sell products with a Nordic impact. The collected data constitutes relevant intelligence, which we analyze and cross-reference to detect patterns such as website similarities, to learn if they are connected. Identified patterns are used to identify and select high priority targets, such as organized large-scale illegal actors.

The NCP Blacklist was initially launched in late 2015 and final deployment took place in early 2016. As the threat landscape continues to change and develop, so does the technical backend of the NCP Blacklist.

Using 2016 as baseline, we have seen NCP IPTV Blacklist numbers rise 179% and 274% respectively for 2017 and 2018 as seen below in figure 8..

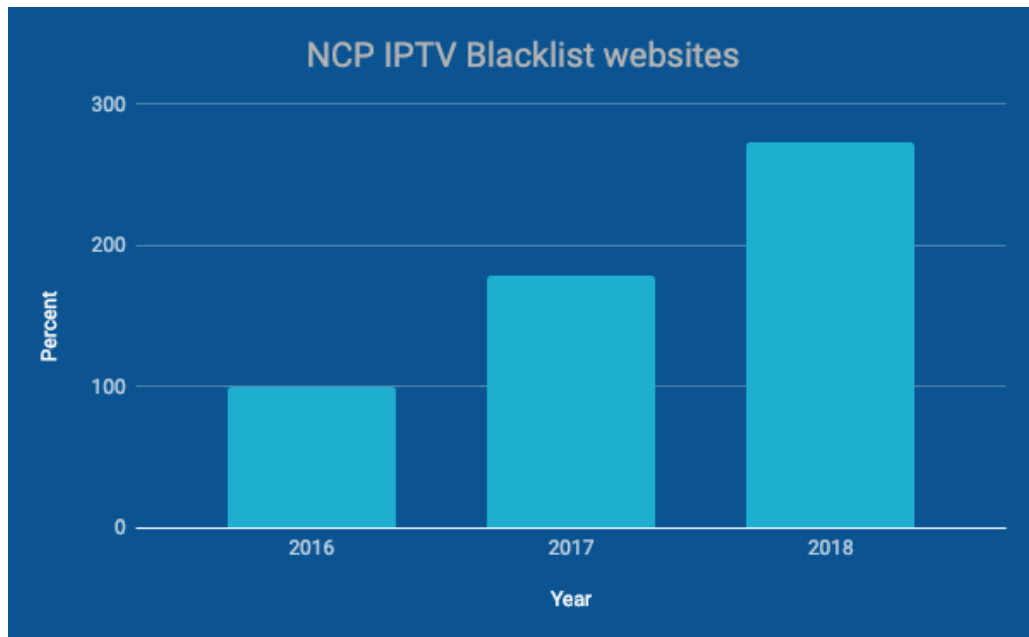


Fig. 8.

IPTV website domain names and registration

The NCP Blacklist is dynamic as new websites are added and existing sites reviewed, and potentially removed continually. To be as effective as possible, the detection systems are optimized to detect the websites as early after launch as possible.

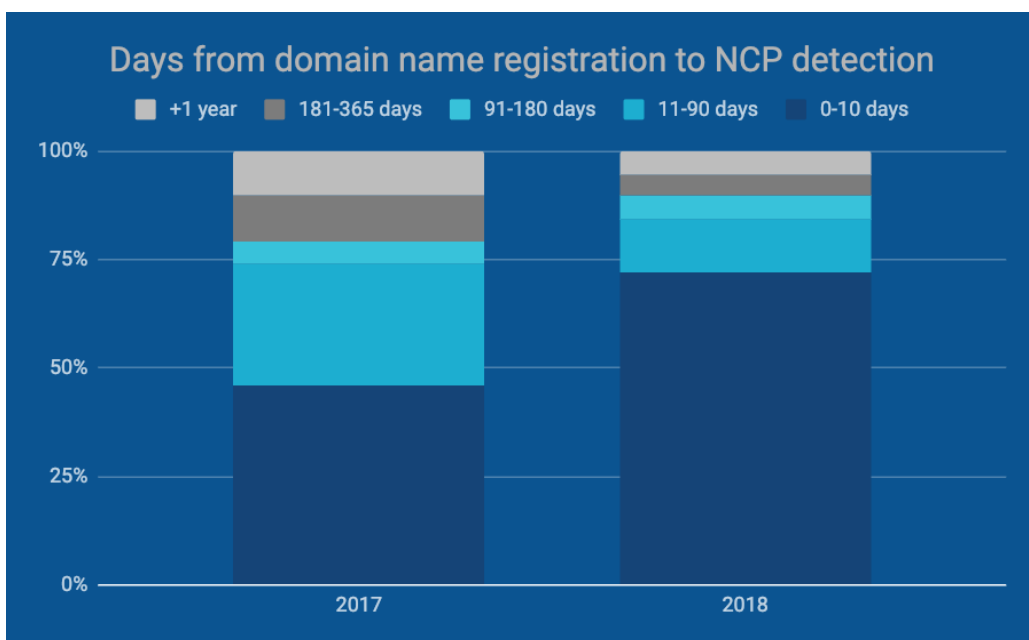


Fig. 9.

As seen in Fig. 9, NCP detected 72% of the blacklist websites within 10 days in 2018. This allows NCP to react swiftly if needed, and NCP members to have available the most complete set of intelligence data possible.

Another pattern related to website activity reveal that registration of domain names to be used for selling illegal IPTV happens more frequently during the winter months and less in the summer as seen below in Fig. 10.

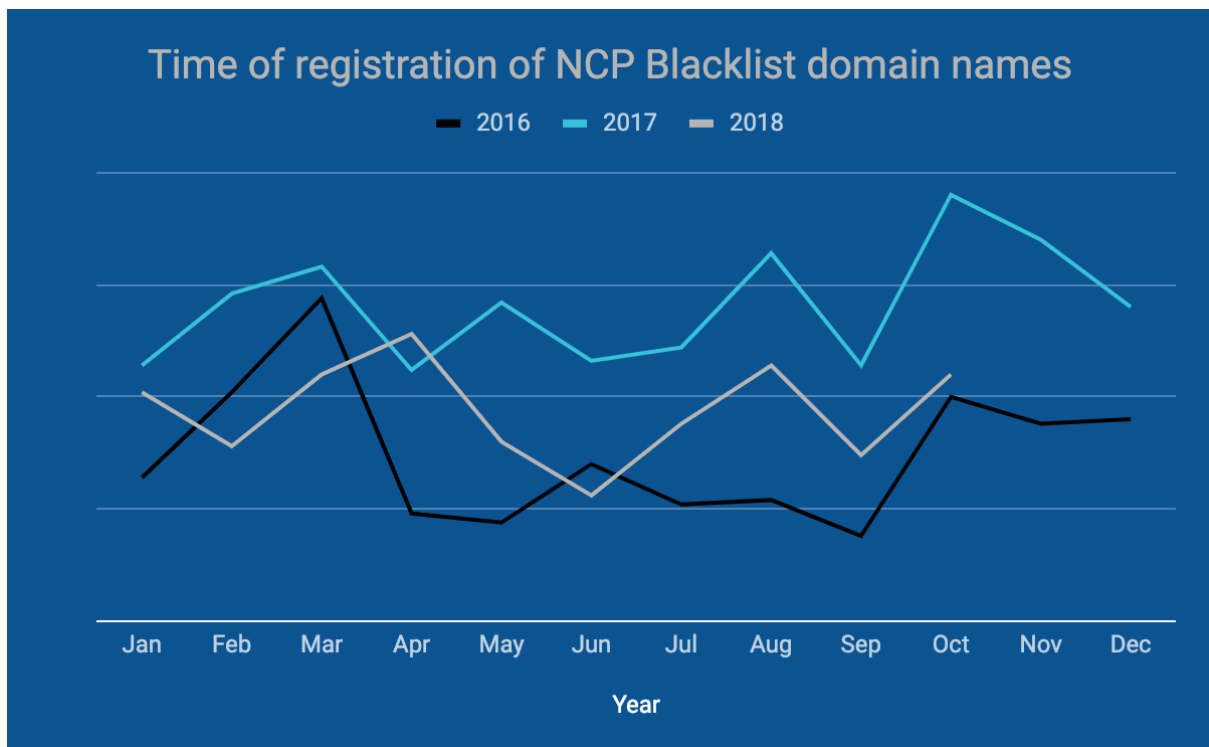


Fig. 10. Note that data from November and December 2018 was not available at the time of writing.

Winter months (in this case in the Nordics/Europe) are traditionally popular “TV months”, which is likely the reason for this activity pattern. Another simple explanation could be that the providers themselves are less active during the summer period.

In regards to which top-level-domains are used by the websites currently in the NCP Blacklist, the following information is available.

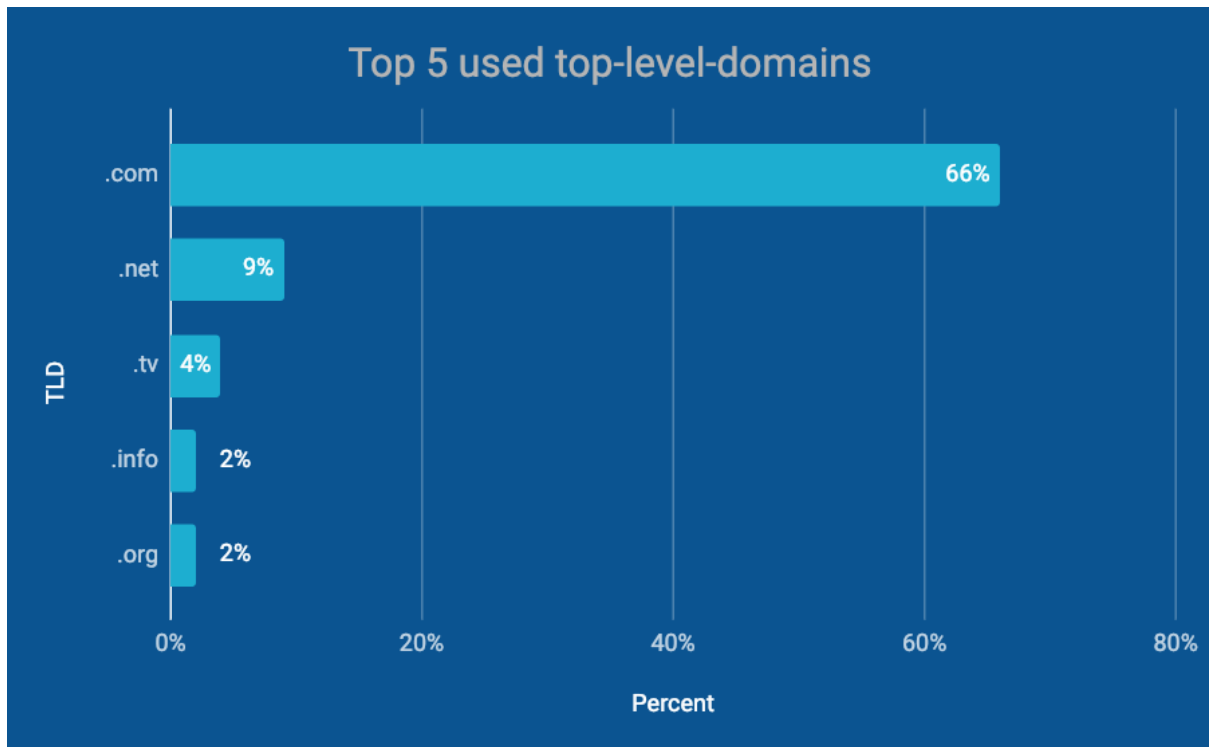


Fig. 11.

A clear majority of the websites use popular generic top-level-domain, such as .com. However one country code top-level-domain makes it into the top 5, namely the .tv domain (country: Tuvalu). Popularity for .tv is obviously tied to the fact that it is the well known abbreviation of the word 'television'. The .tv domain is administered by Verisign in the US, who among others also administer .com. Only 1% of websites in the NCP Blacklist make use of Nordic country code top-level-domain names. Similar with the situation for CS servers, the reason for this is years of effective enforcement within Nordic jurisdictions.

Knowledge of top-level-domain administration and regulation is a valuable tool when it comes to enforcement, as it differs from domain to domain. In some jurisdictions enforcement can be straightforward on the registry level, while others are more complicated.

When we look at domain name composition in the NCP Blacklist, we find that 77% include IPTV in some way or form.

IPTV website hosting

Hosting a website today is very straightforward. Websites available on the open Internet are generally hosted by third party companies, as opposed to individuals setting up a server and hosting the website themselves. Even though the latter option would reduce some risks related to online criminal activities, the convenience from using the services offered by commercial hosting companies are a strong incentive for using third parties. Additionally it is also somewhat cheaper.

Many larger hosting providers double as domain name registrars, and many customers, including those hosting illegal IPTV websites, choose to simply host their websites with them after registering the domain name. For this reason we see some of the largest hosting providers in the world, when we look at information about the the NCP Blacklist websites.

However, in addition to using traditional hosting providers, 18% of websites in the NCP Blacklist make use of CloudFlare services⁶ to attempt to mask or hide their actual hosting information.

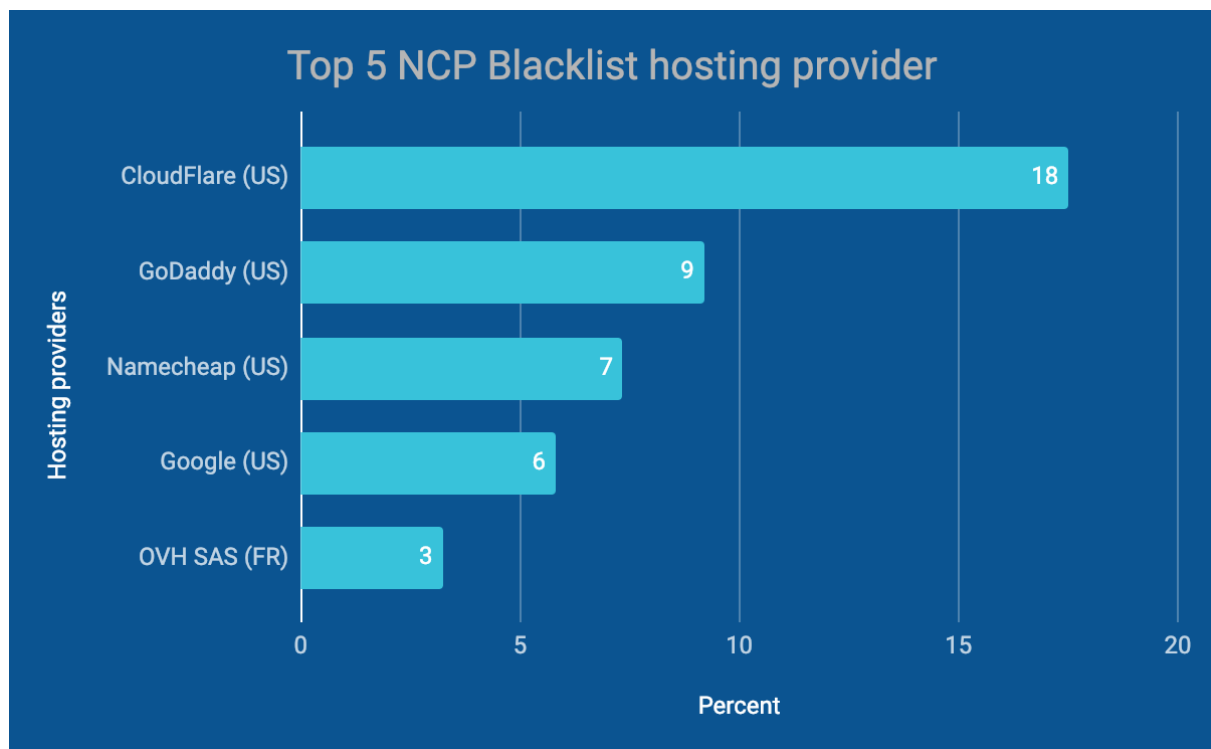


Fig. 12.

Hosting providers from the US dominate the top 5 here as seen in Fig. 12. Still it is important to understand, that the websites using the CloudFlare services are not necessarily hosted in the US. They could be hosted anywhere in the world, and experience shows that they usually follow the general pattern for hosting countries described below.

⁶ CloudFlare is an American company offering a range of Internet services. One CloudFlare service acts as a 'reverse proxy', which allow website hosting details (DNS) to point to CloudFlare network infrastructure instead of the actual point of hosting, effectively hiding those details.

The popularity of the US hosting providers is visible when converting the data into a top 5 hosting countries chart.

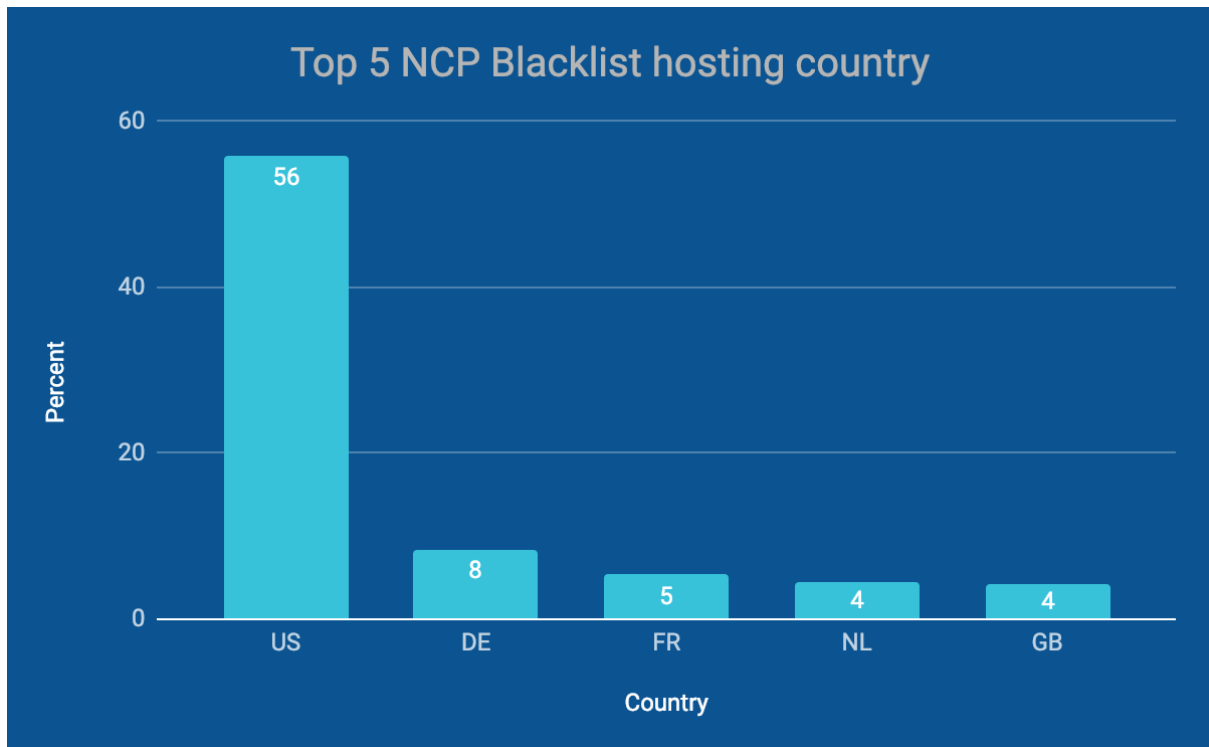


Fig 13.

Here it should also be noted that websites using CloudFlare constitutes 31% of the total websites registered with US hosting providers. This could potentially lower the percentage to 38% for US in Fig. 13, if all the CloudFlare using websites was in reality hosted elsewhere, still leaving the US as the most popular hosting country.

List of figures:

Figure 1: Card Sharing servers

Figure 2: Card-sharing hosting countries 2015 - 2018

Figure 3: Card-sharing hosting countries 2015 - 2018 (heatmap)

Figure 4: CS servers in the Nordics versus globally

Figure 5: Active CS servers in the Nordics

Figure 6: Top 5 Internet Service Providers - CS server hosting 2015 - 2018

Figure 7: Current top 5 CS hosts for the Nordics

Figure 8: NCP IPTV Blacklist websites

Figure: 9: Days from domain name registration to NCP detection

Figure: 10: Time of registration of NCP Blacklist domain names

Figure: 11: Top 5 used top-level-domains

Figure: 12: Top 5 NCP Blacklist hosting provider

Figure: 13: Top 5 NCP Blacklist hosting country