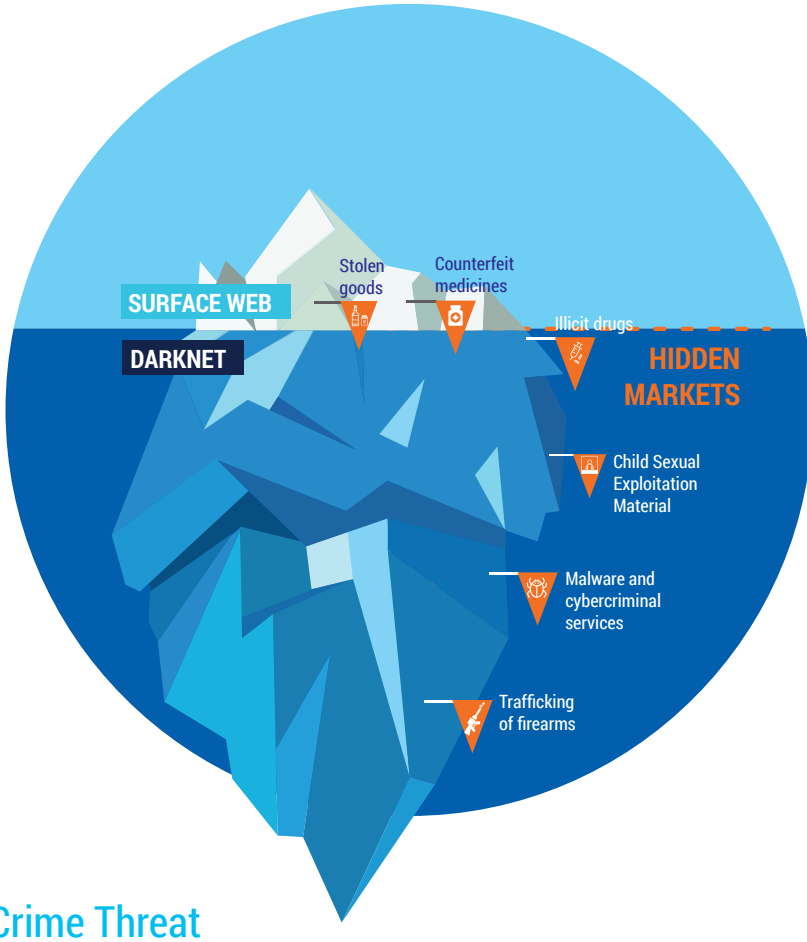
INTELLECTUAL PROPERTY CRIME ON THE DARKNET

Intellectual Property (IP) crime is committed when someone uses an intellectual property right without the authorisation of its owner. **Counterfeiting** and **piracy** are terms used to describe a range of illicit activities related to Intellectual Property Rights (IPR) infringement. Most counterfeit goods infringe a trademark, which means that a good is produced without the authorisation of its rights holder. Piracy refers to the illegal use of literary and artistic works protected by copyrights.

Organised Crime Groups (OCGs) are increasingly involved in the violation of IPR.

WHY IP CRIME MATTERS TO YOU

Criminal activity in this area brings potential harm to the consumer health and safety. Health dangers are not only associated with counterfeit food or pharmaceutical products but also substandard clothing, dangerous electronics or even toys. IP crime also affects the environment. Counterfeit pesticides often contain toxic substances that may contaminate soil, water and food. Last but not least, this crime affects the legitimate economies and results in reduced revenues of the affected businesses, decreased sales volume and job losses.



ONLINE TRADE

Illicit goods and services are increasingly advertised and sold online. Online marketplaces, both on the surface web and Darknet, are used by criminals to purvey a wide range of illicit commodities, such as drugs, firearms, malware, Child Sexual Exploitation Material (CSEM), counterfeit currency, and goods infringing IPR. Those of a more serious nature, such as firearms, are typically placed deeper in the Darknet and often enable further criminality across many crime areas.

> The Europol's Serious and Organised Crime Threat Assessment (SOCTA) 2017 identified online trade in goods as a cross-cutting threat and one of the engines of organised crime.

DARKNET MARKETS

In June and July 2017, two of the largest Darknet markets - AlphaBay and Hansa - were taken down in an international operation, led by the Federal Bureau of Investigation (FBI), the US Drug Enforcement Agency (DEA) and the Dutch National Police, with the support of Europol and a number of other law enforcement partners.

Prior to its takedown, AlphaBay, the largest market, reached over 200 000 users and 40 000 vendors. There were over 250 000 listings for illegal drugs and toxic chemicals, and over 100 000 listings for stolen and fraudulent identification documents (IDs), counterfeit goods, malware and other computer hacking tools, firearms, and fraudulent services. Since its creation in 2014, transactions concluded in the market were estimated to have netted USD 1 billion. Hansa was the third largest criminal marketplace on the Darknet, trading similarly high volumes of illicit drugs and other commodities.

After takedowns, criminals typically shift to existing alternative or new Darknet markets.

Europol Press Release, 20 July 2017

The **drug** market was the largest criminal market on the Darknet. As of June 2017, AlphaBay had over 250 000 separate listings for drugs, accounting for almost 68% of all listings and generating huge financial gains. Some of these represented pharmaceutical products (especially lifestyle medicines) that may have been counterfeit.

Compromised data typically constitutes the second or third largest category of listing on most Darknet markets. However, this activity is not limited to the Darknet. A large number of websites selling compromised card data are also available on the surface web.

Cybercrime tools and services, such as exploit kits, botnets and malware, and Ransomware-as-a-Service, are also increasingly sold on the Darknet. On AlphaBay there were over 75 000 listings for such products and services by the end of 2016, a 25% increase from the start of the year.

Only a few markets openly list **weapons** as a category of commodity sold on their sites. For those that do, weapons typically account for less than 1.5% of their total listings[1].

IPR infringing products sold on the Darknet include counterfeit and pirated goods. There is no specific category for such products on criminal markets and they are typically placed, together with genuine goods, within different (sub) categories, such as Accessories, Clothing, Counterfeit, Digital, Drugs, Electronics, Entertainment, Jewellery, Pharmacy, Software or Others. Categories vary from one Darknet marketplace to another, which makes it a challenge to measure the overall scope of the IPR infringing material on the Darknet.

Counterfeit products alone are estimated to account for between 1.5% and 2.5% of listings on Darknet markets[2]. For instance, on AlphaBay, there were approximately 10 000 listings under category Counterfeits. The most commonly listed counterfeit products on the Darknet are those which are obviously illegal - counterfeit banknotes and fake IDs.

The majority of counterfeit and pirated products continue to be sold on the surface web, on major, widely available and trusted platforms, or by online pharmacies. The sellers present them as, or mix with, genuine products, aiming to reach out to a large number of potential customers.

[1] Europol's Internet Organised Crime Threat Assessment (iOCTA) 2017

[2] iOCTA 2017

BROAD RANGE OF IPR INFRINGING PRODUCTS

There is **a wide range of products[3] infringing IPR** available on the Darknet, such as:

- Clothes, textiles and accessories (e.g. sunglasses, belts, bags, pens)
- Electronics including mobile phones
- Jewellery
- Pirated software (e.g. Adobe Photoshop, Microsoft Office Suites, games, various antivirus software)
- Pirated e-books
- Pharmaceutical products (especially lifestyle medicines, steroids and hormones)
- Subscriptions to TV channels, music platforms, online game accounts
- Watches

BUSINESS MODEL

Darknet markets are large, diverse and increasingly easy to access and use. They allow criminals anonymity and offer possibilities for poly-criminality (trade in various types of illicit goods and services), at the same time generating substantive profits. Darknet marketplaces are also increasingly attractive to criminals involved in IP crime.

Darknet markets resemble the markets available on the surface web. They are typically user-friendly, enabling vendors to use various marketing techniques to increase the profits. Products are displayed in different (sub) categories, along with additional information such as the vendors' profile, ratings, customers' feedback, number of placed orders, average volume per order and prices, often available in different currencies. Buyers can participate in lotteries (to bid for a product) or subscribe to offers.

WHO ARE THE VENDORS?

Criminal vendors involved in IP crime seem to be both lone offenders, trading in small amounts, and members of OCGs

They are profit-oriented, aiming to reach out to a large pool of customers and increase the sales volume. In order to do so, **vendors tend to advertise their products on different Darknet markets** (often using the same user name and selling the products for the same price) **but also on the surface web.**

Vendors appear to specialise in selling one category of counterfeit goods such as (counterfeit) pharmaceutical products or counterfeit luxury goods. However, there are a few exceptions where sellers offer a broad range of illicit products.

One identified vendor sold a broad range of counterfeit products on different Darknet marketplaces, under different nicknames. Beside counterfeit clothes and accessories, the vendor offered counterfeit medicines. The prices of the offered products varied from EUR 50 to EUR 300 and were shipped from the UK worldwide. The vendor had total revenue of over EUR 10,000 and nearly 2,500 comments with positive feedback. The vendor was selling the illicit goods on both Darknet and the surface web.

WHAT ARE THE PROFITS?

It is difficult to determine the overall profits stemming from the trade in IPR infringing material, as the majority of vendors offer a wide scope of products and often on different markets.

The price for counterfeit goods is typically 1/3 lower than for the genuine products. For instance, the price for counterfeit Rolex watches offered on Hansa market varied from EUR 40 to EUR 200.

Prices for pharmaceutical products also vary. One identified vendor sold large amounts of (possibly counterfeit) Xanax, making an overall profit of EUR 152 000.

Pirated software or e-books usually cost, depending on the vendor, about 1/6 of the price charged for the original product.

Some criminal vendors on Darknet markets were reported to have sold on average between 500-1,500 products since they joined the market, with top vendors reaching over 6,000 sales.

Payment is prevailingly done by bitcoin but other cryptocurrencies are also used.

[3] The products are listed in alphabetical order. It is important to note that not all advertised products are counterfeit. Stolen goods, e.g. jewellery, are also often sold on Darknet markets.

DISTRIBUTION CHANNELS

The growing online trade, including in IPR infringing products, is closely related to the **increasing use of parcel and postal services** to import and distribute such goods. The high-frequency, low-volume traffic is one of the features of this crime area.

Some vendors include the source of IPR infringing material in the description of a product. For instance, China is allegedly named as a source for counterfeit clothes; India, US, UK, or Canada for counterfeit medicines or steroids. Hong Kong often appears as a place of shipment, and is followed by countries like Germany, Netherlands, Poland or Ukraine, or generally the region "Europe". The majority of products can be delivered worldwide, with some exceptions only available to specific countries.

An average delivery time advertised by vendors on the Darknet was 4-9 work days. Criminal vendors sometimes even offered discounts for the next purchase or an extra free shipment should the parcel be lost or seized by the law enforcement authorities. No reimbursements were offered for deliveries to specific countries, suggesting higher risks of seizures.

FUTURE FOR IP CRIME ON THE DARKNET

IPR infringing material will continue to be increasingly sold on both the surface web and Darknet. Vendors are profit-oriented and will look out for a large clientele online.

> Currently, trade on the Darknet is limited but it affects a broad range of products. It has however a significant potential for growth.

Darknet markets are becoming more attractive for both criminal vendors and buyers. They allow for anonymity, a poly-criminal environment and high profits. For potential customers, they offer a wide range of commodities and services and are increasingly user-friendly, easier to access and browse through.

In addition, **certain measures taken on the surface web against the IP crime, such as frequent monitoring of online marketplaces, may prompt criminals to move the trade into the Darknet**. At the same time, the recent law enforcement operation targeting Darknet markets has also shown that those marketplaces are no longer beyond control/impunity. Future trade on the Darknet may increasingly migrate from large marketplaces into new, often smaller ones.

Illicit goods, including counterfeit goods, will continue to be distributed via parcel and postal services; however, the concealment and shipment methods may become more sophisticated to increase anonymity and avoid detections.

NEXT STEPS

Knowledge gaps regarding the Darknet trade in IPR infringing material remain. The involvement of organised crime in such trade and a potential for poly-criminality of vendors need to be further explored. Vendors are only one part of the entire supply chain. Buyers, suppliers and any other actors involved in the illicit trade also require special attention. All need to be better analysed in order to develop a clear and complete intelligence picture of the mechanisms of Darknet trade.

It is very important to regularly monitor and understand emerging threats presented by the Darknet, including with regard to IP crime. In addition to patrolling of the Darknet markets, an effective law enforcement response requires a holistic approach and strong cooperation, also with intermediaries such as payment card providers and shipping companies, awareness raising and expertise sharing among investigators responsible for all crime areas represented on the Darknet.

Eisenhowerlaan 73, 2517 KK
The Hague, the Netherlands