In the Shadows of the Internet

Child Sexual Abuse Material in the Darknets

Rob Wainwright, the Director of Europol, opened the European Serious & Organized Crime Conference 2015 in Brussels by noting that anything can be bought and sold in the Darknets[1] with virtually no risk to be caught. Darknets are an increasing priority for law enforcement because they harbor illegal markets of narcotics, stolen credit card information, and services of career criminals like hackers, weapons dealers or counterfeiters. Despite the fact that majority of Darknet users show adverse opinions about child sexual abuse material (CSAM), the common philosophy adopted in this underground of the Internet propagates complete rejection of any censure. Therefore, markets and forums dedicated to CSAM also find a refuge in the Darknets. Although public P2P networks still see the largest volumes of CSAM distribution, more security-conscious offenders in the recent years frequently chose Darknets over other technologies to collect and exchange CSAM. Consequently, markets and forums containing CSAM have found a safe haven in the Darknets and even make up 80% of their traffic according to a recent study.[2]

This analysis will focus on the hidden side of the Internet in relation to CSAM. After resituating the Darknet in the reality in which it rose, the analysis will address the specific use of the "dark" Internet in the context of commercial exploitation of children as well as the obstacles encountered by law enforcement in the fight against this phenomenon.

I What is a Darknet?

In 2001 Michael K. Bergman compared Internet to the ocean: "Searching on the Internet today can be compared to dragging a net across the surface of the ocean. While a great deal may be caught in the net, there is still a wealth of information that is deep, and therefore,

[1] The Darknets are a small part of the invisible web that was intentionally hidden. Two typical darknet types are friend-to-friend networks (usually used for file sharing with a peer-to-peer connection) and anonymity networks such as Tor via an anonymized series of connections, available at: https://en.wikipedia.org/wiki/Darknet_(networking).
[2] http://www.theguardian.com/technology/2014/dec/31/dark-web-traffic-child-abuse-sites

missed"[3]. Fifteen years later and, despite the extremely rapid development of new technologies, Bergman's assessment still holds true. The Deep Web[4] and Darknets are invisible for the great part of Internet users.

"Darknets exploit the infrastructure of the Internet but stand apart from it"[5] – this is one of the most accurate definitions of this reality. As a section of the greater Internet underground, Darknets have several characteristics that define them: they use decentralized anonymizing technology, which bases itself on the infrastructure of the Internet but in such a way that they operate separately from the common Internet traffic and are unreachable for a regular Internet user[6]. Some of the well-known Darknets are Freenet, Tor and the Invisible Internet Project (I2P). It is not one big Internet network but rather multiple groups that are further split by the purposes of those groups, languages and alliances. Whatever the activity, Darknets provide shelter to their users by guaranteeing anonymity.

Originally created in 2002 by the US Naval Research Laboratory, Tor[7] is today run by volunteers and has far surpassed the original uses of the network. Accessible through a correctly configured Tor browser bundle, it permits the publication of completely anonymous web pages inside the network. Pornographic content in this network is abundant and classified according to the preferences of the users. Subcategories such as "hard candy" or "jailbait" can be found. The first term is usually used as an alternative name for CSAM depicting prepubescent children, while "jailbait" is a slang term meaning attractive teenage girl.

Freenet[8] is another popular Darknet created in 1999 by Ian Clarke. Even though Freenet is created using different technological solution from Tor, the final result is similar – a guarantee of anonymity on the Internet and bypass of Internet censure. CSAM here is mixed with all sorts of other material: blogs, archives, political manifestos, and pirated content.

---

[3] Bergman M.K. (2001). White Paper: *The Deep Web. Surfacing Hidden Value*, in «The Journal of Electronic Publishing», 7 (1), http://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main

[4] The invisible web or hidden web refers to the part of the web that is not directly accessible to traditional search engines. It includes all documents not indexed by search tools like Google, Safari, Yahoo, etc.: sources whose access is controlled by a password, sites having an internal database, pages accessed through a search form, unreferenced documents (intentionally or not), intranets, extranets, ...

[5] Mansfield-Devine S. (2009), *Darknets*, «Computer Fraud & Security», 2009 (12), pp. 4-6.

[6] Ibidem.

[7] https://www.torproject.org/

[8] https://freenetproject.org/

Freenet also has its own P2P application, Frost, which allows quick and simple file sharing and communications between multiple users at the same time. Frost boasts several dozen chatrooms dedicated to CSAM exchange.

Sites dedicated to distribution and exchange of CSAM vary from image boards (the so-called "chans") to discussion forums. These may be organized in various ways: from the most simple distinction of material depicting girls or boys, to an elaborate organization between video or photographic material, types of CSAM, producers, the image sets or an appearance by a particular child. Single images are made public directly as attachments to a message, while video material and image archives are more often uploaded to online file hosting services (*cyberlockers*). The link to this material with corresponding password then is made public on the discussion forums or by other means, often together with a couple of "samples" in the form of several attached photographs or screenshots.

II Child sexual abuse material in the Darknets: an established trend

The obscurity of the Darknets is exactly what attracts many illegal activities, including CSAM distribution. More and more CSAM exchange is moving away from the open Internet, led by the motto "security through obscurity". Due to this and the tireless efforts of concerned NGOs and law enforcement, the possibility to just stumble across CSAM by simply browsing the Internet is becoming very small. Consequently, sex offenders are taking refuge in the least visible part of the Net. Contrary to what one might think, the user guide for Darknets is quite easy to find and this CSAM market is easily accessible.[9]

European law enforcement experts estimate that only a small part, around 7-10%, of CSAM online is commercial[10]. However, the assessment of current commercial child sexual abuse trade by the European Financial Coalition against Commercial Sexual Exploitation of Children Online also states that a marked change is being noticed and that this change is primarily driven by Darknet users. The traditional distinction was of commercial trade of CSAM

[9] EUROPOL, « Virtual Global Taskforce Environmental Scan 2012 », p. 16, available at: https://www.europol.europa.eu/content/virtual-global-taskforce-environmental-scan-2012

[10] European Financial Coalition against Commercial Sexual Exploitation of Children online "Strategic Assessment of Commercial Sexual Exploitation of Children Online", 2015, pp. 5-6, available at: http://www.europeanfinancialcoalition.eu/private10/images/news/pdf/65.pdf

primarily in the hands of profit-driven individuals without or with limited sexual interest in children, while individuals with exclusive or primary sexual interests directed at children would rarely participate as commercial actors.

This traditional separation is now changing. Indeed, given the exponential rise in demand for new materials and thus of their intrinsic commercial value, the second category of individuals has become increasingly entrepreneurial, reselling rather than exchanging these new images.[11] This development is worrisome because the demand for CSAM does not show any signs of decrease. On the contrary, with the spread of Internet access worldwide, a corresponding increase can be expected in the future. This means that the incentives for child sexual exploitation, as well as production and distribution of CSAM can be expected to increase.

At the same time, even after some notorious law enforcement operations (such as the take down of Freedom Hosting or Operation Onymous[12]) carried out in the Tor network, it does not seem to affect Tor's popularity for CSAM exchange. On the contrary, with an increasing range of devices, which can facilitate connection to this Darknet, Tor will continue to be the network of choice for CSAM distribution and download.

III The challenges that the Darknets pose to combating CSAM online

National, European, and international law enforcement face continuous struggles to shut down illegal operations in the Darknets. This is due to the technologies on which these networks are based, as they are designed specifically to protect the anonymity of users and publishers of content. Cryptocurrencies used to pay for commercial child sexual exploitation and CSAM in the Darknets are also problematic for law enforcement: Bitcoin[13] and its variants, such as Litecoin and Zetacoin, can exchange hands globally with minimal possibility to trace it back to the original owner[14]. The combination of these two factors, namely an

[11] Ibidem.
[12] http://www.janes.com/article/47455/law-enforcement-struggles-to-control-darknet
[13] A cryptocurrency is a peer-to-peer decentralized electronic money whose implementation is based on the principles of cryptography to validate transactions and generate the money itself https://bitcoin.org/en/
[14] http://www.janes.com/article/47455/law-enforcement-struggles-to-control-darknet

anonymous environment on the Darknets and the use of cryptocurrencies that are difficult to trace results in a relatively risk-free environment for offenders.

Another big challenge is the live streaming of abuse – an offence that leaves very little evidence if it was not intercepted at the time of the transmission or recorded. Many countries have identified the possession of CSAM as a criminal offence but only a few have also included the "knowingly gaining access to" in the definition. The difference of legal wording is crucial in case of live streaming of sexual abuse (via Skype for example) as the material is not being downloaded into the possession of the user. Nonetheless, the material is being accessed and, in some cases, remotely directed.

In addition, and still at the legislative level, in the majority of cases the victim and the offender are present in different legal jurisdictions, so the success of investigations related to CSAM will depend on the harmonization of legal definitions, cooperation procedures, and communication between different law enforcement authorities.

The lack of evidence generated by the live production of CSAM is a major obstacle for the identification and location of victims in order to protect them from the abusive environment in which they develop. Each new piece of CSAM content means that a new child is a victim of sexual abuse. Law enforcement and non-governmental organisations (NGOs) have therefore as a priority the identification of these victims from clues found in the materials (a specific object in the room, a clothing brand, etc.). However, this analysis must rely on a recording.

The remaining vulnerability to be exploited by law enforcement is human error: a lot of the arrests related to the Darknets were determined not by the technological capabilities of law enforcement to trace the individuals but by the fact that people become less cautious over time and give out information about themselves, which ultimately leads to their identification[15].

[15]David Glance „Despite Darknet drug market arrests and seizures, can they be stopped?“: http://theconversation.com/despite-darknet-drug-market-arrests-and-seizures-can-they-be-stopped-33867
http://www.wired.com/2013/10/thompson/

IV Conclusion

CSAM markets online are known for dynamically changing their platforms of communication and technologies to those perceived as most secure. Darknets – the hidden layer of the Internet unknown to the majority of regular Internet users, represent just the latest step in this evolution. They are proving to be a permanent challenge for law enforcement: the anonymisation and encryption functions of the Darknets, together with the cryptocurrencies used in these networks to pay for illegal material, the lack of evidence in the case of live streaming of sexual abuse and, finally, the international nature of this crime, are impeding the identification of criminals and the victims. Although these technologies are also used for completely legitimate activities, the resentment of any type of censure in this medium provides an ideal space for CSAM distribution.

As long as the traditional tools of law enforcement are not very effective in the Darknets, we need to find completely novel ways of combatting the diffusion of CSAM. A closer cooperation with non-governmental and all other actors on the front lines is absolutely necessary for tackling the issue in a more creative way, as shown by the Sweetie case[16] or Microsoft's Photo DNA[17].

This analysis was written in June 2015 by Justė Neverauskaitė and reviewed by ECPAT Belgium.
ECPAT Belgium is the Belgian member of ECPAT International (End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes). The mission of ECPAT Belgium is to fight against sexual exploitation of children for commercial purposes: child prostitution, child pornography, trafficking of children for sexual purposes and child sex tourism.

ECPAT Belgique
Rue du Marché aux Poulets, 30
1000 Bruxelles
Tél: 02/522.63.23
Email: info@ecpat.be

[16] See ECPAT Belgium, "Child Sexual Abuse Material and the Internet (part 2): Challenges for the Law Enforcement Agencies", June 2015, p. 2.
[17] Hash value is an alpha-numerical code generated by an algorithm; this code is often used in computer forensics to identify files with certainty. http://www.zdnet.com/article/microsoft-joins-the-fight-against-child-pornography/