ACUMINOR

Online Sexual Exploitation of Children

How understanding and tracing of transactions can save victims

relations@acuminor.com
www.acuminor.com

Report 2018:2

Acuminor
REPORTS

In the Philippines, a mother sexually abuses her little girl for EUR 10-60. Through a chat forum, a man in Denmark is providing instructions as he watches the abuse in real-time via webcam.

In Spain, a young girl is crying as she gets undressed. A man from Germany is threatening to kill her family if she does not send him sexual material. In Finland, a teenage girl discovers that her private pictures have been stolen as she is contacted online by a man from Belgium, extorting her for money.

This is the agonising reality for many children in the world, and online sexual exploitation of children takes many different forms.

Internet, an extended hunting ground

Adult attraction and sexual abuse of children have occurred throughout human history. In the 1850s, the first publication dedicated solely to child sexual abuse was published, but it was not until the 1970s that widespread public awareness of the matter was recognised in the West.

At that point, physical contact needed to be established by the perpetrator, delimiting the range of potential victims. Modern technology have replaced the need of this physical presence. Rapid technological developments in conjunction with anonymization tools and encryption on e.g. darknet offers a clandestine and worldwide platform for perpetrators to connect with each other, and to share and trade material.

"Live-streamed abuse is when a perpetrator directs an abuse online to fit their preferences"

Putting the pieces together

Crimes in the digital era often constitute a substantial challenge for law enforcement agencies, that struggle to stay ahead of perpetrators and shed light on their course of action. Thus, collaboration and information sharing are crucial. Intelligence have identified numerous different risk factors linked to perpetrators and victims, e.g. age, country of residence and money flows. In fact, money flows vary depending on the type of online sexual exploitation, i.e. live streaming and sextortion. Knowing how, where and to whom these transactions are made can play an essential role in discovering sexual abuse online.

Live streaming

Live-streamed abuse is when a perpetrator directs an abuse online to fit their preferences. The orders are usually communicated via a chat forum while the abuse is streamed via webcam in real-time. This crime involves three parties, the perpetrator with a sexual interest (ordering the abuse), the perpetrator with a financial interest (conducting the abuse), and a child (the victim). Transactions are often made via money transfer services, the regular banking- and online payment system, and prepaid cards. Together with relevant customer and geographical factors, the following are examples of transaction indicators for live stream sexual abuse:

- Card payment to an online payment solution shortly followed by an outgoing transaction
- Amounts does not in general exceed EUR 60
- Low value transactions to the same recipient (financial interest perpetrator)

There are indications that it exists a relationship between live streaming and travelling to a country to commit hands-on abuse. I also happens that a perpetrator has travelled to a country and maintained contact with the abused party upon return, in order to obtain abuse material or access live streaming.

Sextortion
Sextortion, to extort someone into sending content of sexual character by using threats, have increased rapidly. Nearly 70% of the European countries have reported cases of sexual coercion or extortion of minors. Adults who are affected are often forced to pay, whereas affected children are primarily controlled to produce more material. Perpetrators of sextortion can be very persistent and continue their threats for months or years. Transactions are often made via the regular banking system or virtual currencies.

Together with relevant customer and geographical factors, the following are examples of indicators for sextortion:

- Single or numerous outgoing transactions to the same recipient (perpetrator)
- Single or numerous incoming transactions from one or multiple senders (victims)

What can you do to help?
In EU there have been relatively few convictions of live streaming and sextortion cases compared to the estimated number of offences, but victims have been identified in Canada, the Philippines, Scotland and the U.S.

Recent intelligence has identified an increased presence by organised crime groups in the production and trade of live-streamed sexual abuse and sextortion, crimes they consider a business opportunity. With further collaboration and intelligence work, such networks can be dissolved.

Identifying and understanding the risks from certain transactions and behaviours is a must. Transactions can serve as evidence against a perpetrator and, even more importantly, lead to the identification of a victim.

All parts of society need help each other win the fight against online sexual exploitation of children. Finanical institutions must to make sure that they, as part of their anti-financial crime efforts, do everything in their power to find, stop and report the perpertators. ■

"In order for society to win the fight against online sexual exploitation of children, finanical institutions need to make sure that they do everything in their power to find, stop and report the perpertators"