Executive summary

This Paper introduces the key findings of a study of the distribution of captures of live-streamed child sexual abuse which were publicly available online during 3 months in 2017 ("the Study").

The Study was carried out by Internet Watch Foundation (IWF) and funded by Microsoft. Over a three-month period between August and October 2017, images and videos meeting the research criteria were identified using a combination of leads from existing IWF data and techniques employed by IWF analysts to proactively locate child sexual abuse imagery being distributed online. The images and videos were then assessed in accordance with IWF's standard procedures for processing child sexual abuse imagery. Data captured in each instance included image category[5], site type, commerciality, hosting location, and the assessed age and gender of the individuals depicted.

During the Study, **2,082** images and videos were assessed as meeting the research criteria.

Key findings were:

- 96% depicted children on their own, typically in a home setting such as their own bedroom.
- 98% of imagery depicted children assessed as 13 years or younger.
- 96% of the imagery featured girls.
- 40% of the imagery was Category A or B.
- 100% of the imagery had been harvested from the original upload location and was being redistributed on third party websites.
- 4% of the imagery was captured from mobile-only streaming apps.
- 73% of the imagery appeared on 16 dedicated forums with the purpose of advertising paid downloads of videos of webcam child sexual abuse.

Key recommendations are:

- Recognition of the need for awareness raising programs aimed at educating children and those in a parental role about the risks of live-streaming services;
- Wider implementation of tools to tackle online distribution of child sexual abuse imagery by service providers;
- Development of new services including video hashing technology to detect duplicate captures of live streamed child sexual abuse which have been redistributed online;
- Recognition of legal loopholes facilitating distribution of child sexual abuse imagery and elaboration of policy proposals that can influence positive change.

This paper sets out the limitations on the Study and makes recommendations for further research which can be undertaken to expand upon and clarify the findings. It is hoped that by raising awareness of this issue, a multi-agency approach can be taken to help protect children from the immediate and long-term effects of the distribution of permanent records of their sexual abuse.

[5] The IWF assess child sexual abuse imagery based on the categories detailed in the Sentencing Council's Sexual Offences Definitive Guideline (see https://www.iwf.org.uk/what-we-do/how-we-assess-and-remove-content/laws-and-assessment-levels). These are set out in full at Appendix B.

Key recommendations

The Study identified several opportunities for stakeholder action to prevent and respond to online distribution of captures of live-streamed child sexual abuse. Key recommendations are as follows.

Creation of awareness programs aimed at parents and younger children regarding the risks of online streaming services

Whilst a number of initiatives are in place to educate older children and parents about the risks associated with the production and distribution of images in the context of "sexting", this Study suggests there is still a lack of awareness amongst children of the risks of live interactions via webcam and the potential for permanent records to be created and distributed outside of their control. Additionally, these findings demonstrate the need for awareness-raising initiatives aimed at primary age children regarding the permanence of content distributed online and the potential for loss of control over its removal and onward distribution.

It is recommended that stakeholders working in online child protection seek to implement initiatives which better inform parents, and children of all ages, of the short-term and long-term risks of live interactions via webcam.

Wider implementation of existing solutions to tackle online distribution of captures of live-streamed child sexual abuse by service providers

This Study identified an emerging trend for captures of live-streamed child sexual abuse to be collected on dedicated forums and distributed for the purposes of financial gain. The 16 forums identified in the Study which were dedicated to distribution of child sexual abuse imagery were using captures of live-streamed child sexual abuse to advertise paid downloads of associated video content from third party cyberlocker services. There are often no indications given on the cyberlocker site which would provide an indication of the content of the download and the service may therefore be completely unaware that it is hosting such child sexual abuse imagery.

It is recommended that cyberlocker services take positive action to counter this misuse of their services by using keywords lists and image hash[37] lists to identify and remove such content.

It is also recommended that the payment services industry effectively partners with all available sources of intelligence to ensure it is not inadvertently facilitating the commercial distribution of child sexual abuse imagery by continuing to provide payment services to cyberlocker or file hosting sites which are unwilling to take these steps.

Development and implementation of new solutions including video hashing technology to detect captures of live-streamed child sexual abuse

Offenders publicly distributing captures of live-streamed child sexual abuse online are exploiting premium-only cyberlocker services to monetise such distribution and to frustrate removal of videos at source.

The use of image hash lists using Microsoft's photoDNA are an effective tool to prevent the upload and/or detect distribution of duplicates of child sexual abuse images in online services. Whilst a number of solutions are in development, to date there is no similar industry standard for the detection of duplicative video content. The development of an industry standard method for hashing videos of child sexual abuse would enable videos being redistributed within cyberlockers to be quickly identified and removed by the providers of these services.

Internet Watch Foundation is currently working with Microsoft to develop an industry standard enabling a list of video hashes to be created. Partnering with IWF to implement new solutions will better enable organisations within the internet industry to combat the redistribution of videos of live-streamed child sexual abuse online.

[37] An image "hash" is a unique string of characters generated from the binary data of a picture or video and/or biometric information within a picture. Hashing algorithms such as Microsoft's photoDNA ensure images can be identified using the hash even if the original image has been resized or altered. (http://news.microsoft.com/presskits/photodna/)