Internet Watch Foundation

Briefing Paper – Preliminary Analysis of New Commercial CSAM Website Accepting Payment by Bitcoin

Created	January 2014
Author	Sarah Smith (Technical Researcher, IWF)
Created for	Fred Langford (Director of Global Operations), SMT, Board

CONTENTS

EXECUTIVE SUMMARY

Since June 2013, IWF has observed a rise in the number of reports relating to child sexual abuse material (CSAM) appearing in discrete orphan folders on hacked websites.

This method of distributing content had not been seen in widespread use since approx. 2010, when the use of free-hosting file stores and image hosting websites (aka cyberlockers) became the more commonly encountered method of hosting large volumes of images which are then hotlinked into numerous third party sites. However, the relatively recent emergence of "Hacking as a Service" ("HaaS"), commonly used by distributors of phishing scams and malware, may be an influence on the re-emergence in distributing child sexual abuse content via hacked sites.

On 23rd January 2014, a report was received of a URL relating to a webpage on a hacked website. When the URL was accessed, the webpage automatically redirected to a commercial child sexual abuse website located in a folder on a further hacked website.

Intelligence provided by reporters shows that the URLs which redirect to the commercial CSAM website are being circulated via spam emails.

Commercial child sexual abuse websites are tracked by IWF as part of the Website Brands Project. Since 2009, IWF has identified 1,609 individual Website Brands, which are then further analysed and grouped together based on a variety of criteria including registrant information, common payment mechanisms, hosting patterns and "look and feel" of the webpage. IWF research into Website Brands indicates that there are approximately 10 "top level distributors" responsible for the distribution of all of these websites.

This commercial CSAM distributor is therefore of particular interest for the following reasons:-

- The re-emergence of hacked websites as a method for distributing commercial CSAM websites.
- The commercial child sexual abuse website identified in January 2014 is a "Brand" which has not previously been observed by IWF. Additionally, the website gives no preliminary indicators to link the site with any of the previously identified "top level distributors" of commercial CSAM.
- The format, layout and "look and feel" of the commercial website is one which has not been commonly in circulation since approx. 2010
- The commercial CSAM website is unique amongst the commercial CSAM websites identified by IWF in that it purports to accept payment only in bitcoins.

This paper provides a preliminary analysis of this emergent trend including dissemination method, distribution method and payment mechanisms.

THE SPAM EMAIL

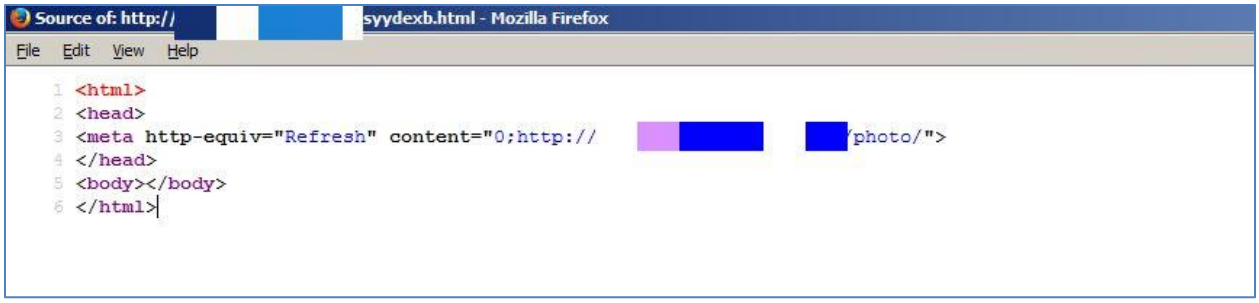
Reporters' comments to IWF state that the URLs of the hacked sites which redirect to the commercial CSAM website were received by them via spam email. Some reporters have also provided a copy of the email text and email headers.

In accordance with data protection legislation, permission will be sought from the reporters to pass their details together with this information to law enforcement for further investigation as they deem appropriate. The current known texts of the email body appear below at Appendix 1.

THE "REDIRECTOR" HACKED SITES

The redirector websites have been hacked with a single .html webpage with an apparently automatically generated name consisting of 7 random characters.

An analysis of the page source (screenshot below) shows that it contains only the instructions required to instantly redirect the user to a third party site hacked with the commercial CSAM website. The only difference between the code on each of the redirector sites is the URL to which the user is redirected.



This is a current and emerging trend. As at time of writing on 24th January, only one day after receiving the initial report, IWF has received reports relating to 6 separate hacked sites redirecting users to third party sites hacked with the newly identified commercial CSAM template.

These sites are diverse in content and hosting location (North American and EU countries) and there is no preliminary indication that the operators of the sites are aware of the abuse of their websites to redirect to this content. The websites are those of small businesses and voluntary organisations and the most likely explanation for these sites being hacked is that they have poor website security and are therefore vulnerable to compromise.

THE CSAM HACKED SITES

As with the redirector hacked sites, the websites which have been hacked with the commercial CSAM website are diverse in content and hosting location (North American / EU)

and are those of small businesses or private individuals. Similarly, no preliminary indications that these sites are complicit in the distribution of this content have been found.

As mentioned above in relation to the "redirector" hacked sites, the most likely reason for these sites having been compromised is poor website security. As is widely known, a number of tools currently exist in the underground market service which, for a fee, automate the process of hacking websites for use in the distribution of criminal material (see for example http://www.webroot.com/blog/2013/07/31/diy-commercially-available-automatic-web-site-hacking-as-a-service-spotted-in-the-wild/).

THE COMMERCIAL CSAM WEBSITE

The commercial CSAM website is previously unknown to IWF. The website differs from other commercial CSAM templates recently observed on hacked websites, which consist of a single page of CSAM images and contain malware downloads.

The CSAM website consists of 9 pages all contained within a single folder – a front page followed by 6 "preview" pages containing images of known victims and a "join" page. The join page indicates that payment for membership of the site can be made only in bitcoins.

The format and production quality of this website is consistent with the type of commercial CSAM websites historically observed but which have not been commonly seen since approx. 2010.

To date IWF have identified 5 websites which have been hacked with this commercial CSAM website.

PAYMENT

This commercial website brand is unique in that it is the first which IWF has encountered on the public web which purports to accept payment only in bitcoins. This is significant as while to date this payment mechanism has not been associated with payment for CSAM within the European Union it evidences concerns long held by law enforcement and experts in the field of online child sexual exploitation that this payment mechanism would become subject to abuse (see http://www.europeanfinancialcoalition.eu/private10/images/document/5.pdf)

Bitcoin is a borderless peer-to-peer cryptocurrency first introduced in 2009. Bitcoin has been widely criticised due to the perception that it is an "anonymous" payment method and because of its apparent association with illicit activity. Bitcoins were for example used to make payment on the notorious Silk Road online black market located within the Tor network.

However, like any form of payment mechanism it is open to abuse by those with criminal intent and while providing a certain degree of anonymity (by identifying those receiving

payment by a Bitcoin address rather than an individual name), it is possible to track the flow of bitcoins to find clues to the identity of the owner.

A detailed examination of the operation of Bitcoin is beyond the scope of this paper but further information is available at www.bitcoin.org.

CONCLUSIONS / RECOMMENDATIONS

The offering of payment in bitcoins by this previously unobserved top level commercial distributor is a newly identified, emergent trend and at time of writing the volume of reports is relatively small. As such, at this stage it is only possible to undertake a preliminary analysis.

IWF will continue to monitor the trend for any increase and perform further research to identify possible links with known top level commercial CSAM brands in order to provide information to law enforcement partners and aid in the disruption of CSAM distribution.

It is also recommended that this paper be circulated to stakeholders including law enforcement, sister Hotlines and payment providers to raise awareness and enable them to undertake further investigations and formulate procedures for tackling this emerging issue.

APPENDIX 1

Sample Spam Email Texts

Young Models Pics Junior Nude Pics

http://xxxxxxxxx.com/xxxxxx.html *[URL REDACTED]*

The next day, all of the grandkids were allowed to go up to see him elan boat model and say our good-byes. I eyes were more adjusted to the dark, but there was still no sign of which way he went. She stayed in bed most of the time, too scared to venture out into this utterly foreign land. These chicks are dressed in their sexy underware for some cookie licking and fingering. Teen, Movies, Free sex movies, Young teen hardcore www.

Free Nonude Junior Models Preteen Nonude

http://xxxxxxxxxxxxxxxxxxxxx.org/jxhodkr.html

For some reasons beyond me, people don't vlad model anya like me' he said. Free Pics and Video Clips Very Cute Preteen Models , Free Picks Of Models 12-17 Y. Wide varieties of shrimps are produced on these farms and most of them are located in Asia. Menchville is a Hell hole! On that ban, when I would try to post it would tell me I was banned, but the reason given was blank. Skinny Girls Nude 62. Other classic feminine names with boyish nicknames that come to mind: Georgiana (Georgie), Josephine (Joey), Martha or Martina (Marty), and of course Samantha (Sam) and Alexandra (Alex). Baron explores the paradox of women's exclusion from political rights at the very moment when visual and metaphorical representations of Egypt as a woman were becoming widespread and real women activists--both secularist and Islamist--were participating more actively in public life than ever before.

GLOSSARY

Cryptocurrency - A digital or virtual currency using cryptography for security. A defining feature of a cryptocurrency is that it is not issued by any central authority, rendering it theoretically immune to government interference or manipulation. The quasi-anonymous nature of cryptocurrency transactions makes them well-suited for a host of nefarious activities such as money laundering and tax evasion.

Cyberlocker – A third party website to which users can easily upload content such as webpages, images, data files or videos enabling others to view or download that content. Also known as "one click hosting" as the content can often be uploaded/downloaded in "one click".

Hotlinking – Displaying an image or video on a website by linking to the same image or video on another website rather than saving a copy of the image or video on the website on which it will be shown.

Orphan Folder – A folder on a website which is not hyper-linked to from anywhere within the parent website.