BRIEFING PAPER - Rogue Affiliates Distributing CSAM using "Disguised Websites" (Public version)

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

TABLE OF CONTENTS

BACKGROUND

In late 2011, the IWF Hotline identified a rising trend in websites which use a referrer-based content method of distributing CSAI. Such websites present different content based on the website (or "gateway") from which the visitor is coming to the site. Thus, when the URL is loaded directly into the browser the page that loads usually contains adult content. However, when accessed via a particular "gateway" site, the actionable content is displayed.

This is a legitimate web development technique designed to improve user experience and can be achieved by a number of methods such as (as in this case) using the value passed in the HTTP REFERER field of the page header, the user agent (i.e. the web browser that is being used) or the IP address of the user in order to present targeted content to the user. However, like any technology of its type it is open to abuse.

This type of content represents a challenge for the Hotline as direct navigation to the URL – which is how Analysts would access URLs contained in public reports - results only in the display of non-actionable content.

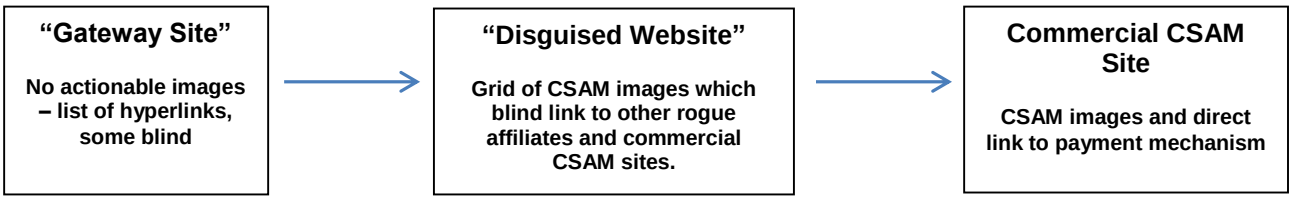
Whilst IWF Analysts are adept at recognising the templates of such sites, without knowledge of the specific referring URL it is often not possible to take any further action. In early 2012, IWF formulated a procedure for manipulating the sites displaying the hidden child sexual abuse content to extend the period of time that this actionable content remains available to view. This procedure has not been published but was successfully implemented in the IWF Hotline processes, enabling the content to be assessed by IWF Analysts and details passed to sister hotlines and law enforcement for removal/investigation. Specific details and training on the procedure for manipulating the disguised websites to display the child sexual abuse material has been made available to our sister hotlines and law enforcement.

IWF is aware of the cluster of "gateway" sites which are usually acting as referrers for the actionable content. These "gateway" sites do not display child sexual abuse material, but form the start of the "digital pathway" to unlock hidden child sexual abuse material on the rogue affiliate sites ("disguised websites") they are linking to. These "disguised websites" are monetised (amongst other methods) by participation in a number of traffic exchange programs and website affiliate programs and therefore use random link scripts to direct traffic to a variety of third party sites, which can make it difficult to quickly replicate the request and re-access the actionable content. An explanation of traffic exchange and web affiliate programs appears below.

During the course of 2013, Hotline has increasingly seen a specific sub-network of these disguised websites providing a "digital pathway" not only to seemingly legitimate websites providing adult content but also to the most prolific commercial child sexual abuse sites identified by IWF within the Website Brands Project.

This paper provides an analysis of the sub-network of disguised websites and their operators, including how the sites are being monetised and legitimate services being abused for the distribution of child sexual abuse material. The paper also examines the disguised websites' connection with the distributors of the most prolific commercial child sexual abuse websites as identified by IWF. It is hoped that this information may be of assistance to law enforcement, providers of payment services and industry stakeholders in disrupting and investigating the activities of individuals attempting to profit from the distribution of child sexual abuse material online.

THE "DIGITAL PATHWAY"



HOW THE SITES ARE BEING MONETISED

Website Affiliate Programs

A website affiliate program is a marketing program whereby an advertiser or merchant recruits affiliate webmasters to place the merchant's banner ads or content on their own website. In the case of adult pornography websites, the merchant will often also make available an amount of free adult content which the affiliate webmaster can place on their website and which provides a hyperlink to the merchant site itself. The affiliate webmaster will receive a referral fee or commission from sales when the customer has clicked a link on affiliate website to get to the merchant's website and performed the desired action, usually make a purchase.

The most common types of affiliate programs include pay-per-click (i.e. commission is paid whenever an ad is clicked and redirected to the merchant site regardless of whether a further action is then performed by the user), pay-per-lead (i.e. commission is paid where the user subsequently downloads a file or fills in a contact form), and pay-per-sale (i.e. commission is paid when the user subsequently makes a purchase).

Traffic Exchange

The disguised websites use traffic exchange scripts whereby third parties can submit URLs to receive traffic from adult sites. This technique is most commonly associated with the promotion of adult pornographic content and it is a quick and easy way of driving high numbers of users to websites.

Put simply, traffic exchange ensures users of adult sites will get redirected to other sites using the same exchange program a percentage of the time, rather than getting the content they have clicked on.

The basis of the technique is that the more visitors to a site, the more sign-ups to services which those sites are promoting will be received. Also, the higher the traffic is to a site, the more likely it is to rank highly in search results. This saves affiliate webmasters spending time and money on traditional SEO.

Adding a URL to the exchange program on a particular site is generally as easy as clicking a link on a site using the program and submitting the URL. As most programs are largely unregulated the technique is frequently abused to enable the monetisation of CSA content online.

However, in the case of this particular group of disguised websites, the referrals are apparently in a closed loop – clicking on the "Webmaster" link on each of the various affiliate sites takes the user to a 404 page.

THE DISGUISED WEBSITES

TGP Template

The majority of the disguised websites (both the adult and CSAM versions) are in a TGP format and have the same layout – they are all thumbnail gallery sites consisting of a title above a grid of images.

The images when clicked divert the user via a blind link to a third party site. Users clicking on images on the adult version of the site are diverted to content on apparently legitimate adult websites and it is supposed that this creates a payout for the rogue affiliate behind the disguised website on a pay-per-click basis for that referral. However, users clicking on the CSAM version of the site are diverted via a traffic trading script to other disguised websites within the group, third party banner sites linking to or containing CSAM (presumably for traffic exchange) and also to the most prolific commercial CSAM sites as previously identified as part of the Website Brands Project. It is proposed that the purpose of diverting users to the pay-per-view commercial CSAM sites works on the same basis as a traditional website affiliate program as outlined above.

The Paysites

At any given time, approx. 2-3 of the domains operated by this group take the form of paysites. The technique is the same in that the URL must be accessed via a particular referrer website to display the CSAM content, but in this case the monetisation of the site is achieved by directly defrauding a legitimate adult pornography provider by inducing users to make payment via a third party payment provider for what they believe to be CSAM. In actuality, the payment is being made to the adult pornography website and to all intents and purposes will appear to them to be a legitimate sign-up. As part of the website affiliate scheme, the adult site will make a payment to the affiliate (sometimes as much as USD30 per referral).

The user receives membership of the adult site, which contains only legitimate adult content. For obvious reasons they are unlikely to complain(!) so the scam continues undetected. The immediate and real time nature of the payment means it is unlikely to be detected as abnormal by usual KYC or compliance procedures in place at these legitimate payment services and anyone visiting the affiliate site to ensure it is compliant will see only a seemingly legitimate site offering adult content supplied by their customer, the legitimate provider of adult services.

REGISTRAR INFORMATION

All the domains are registered via a specific registrar located outside of Europe. Whilst it is not appropriate to publish these details publicly, this information has been provided to law enforcement for their further investigation as appropriate.

HOSTING INFORMATION

All of the disguised websites are hosted on the servers of a specific European ISP. Whilst it is not appropriate to publish these details publicly, this information has been provided to law enforcement for their further investigation as appropriate.

It is of particular note that the CSAM templates cannot be accessed using an IP address which geo-locates to the country in which the host ISP is based, though if using a proxy to access the sites from a variety of other “locations” worldwide the CSAM content is visible. An analysis of the scripts running on several of the gateway sites shows that a lookup of the IP being used for access is made against a

publicly available online geo-location database and where the IP is listed as being based in the host country, the adult template is returned. This information has been made available to our sister hotline in the host country which now uses a proxy to access and assess these sites and have confirmed that when accessing via a non-host country IP address they can view the CSAM content.

This information should enable our sister Hotline to report the content to both local law enforcement and the hosting ISP allowing further investigation and removal of the content. Whether this technique is being used solely to frustrate attempts to remove the content or whether in fact this provides an indication of the location of those posting the sites in that it deflects a possible investigation by local law enforcement is unclear and may warrant further investigation.

THE ROGUE AFFILIATES

The group of 73 currently identified domains are registered to a group of 5 individuals. Some of the domains have been allowed to lapse and have subsequently been re-registered by other individuals. It is not known but is suspected that the registrant information provided may be false, however the fact that the information is consistent indicates a link between the domains.

Two of the registrants provide the same email address and have very similar names. This is a clear link between these two registrants. Additionally, the nameservers of these domains change very frequently and an analysis of hosting details shows that at one time or another domains belonging to each of these registrants have been using nameservers located at the domains of one of the others.

Full details of the registrant information and identified domains have been passed to law enforcement for their further investigation as appropriate.

CONCLUSIONS / RECOMMENDATIONS

The distribution of child sexual abuse content using this disguised website technique represents a challenge for Hotlines attempting to effect its removal as without knowledge of the referring URL it is not possible to view and assess the actionable material. This ensures that such disguised websites remain active for long periods of time. The disguised website technique also frustrates compliance procedures implemented by providers of payment services, tricking legitimate services into providing service to what is essentially a criminal enterprise.

It is therefore recommended that IWF continues to engage with its Members, affected payment providers, sister Hotlines, law enforcement agencies and the wider online industry to raise awareness of this technique and ensure that steps can be taken to effect removal of these sites and investigation of the distributors behind them.

It is further proposed that the individuals using this technique to defraud the affiliate programmes of legitimate providers of adult websites are also profiting in the same manner by making referrals to dedicated child sexual abuse websites. It is therefore possible that an investigation of payments being made to these individuals by the legitimate defrauded payment providers may provide intelligence regarding not only the individuals behind these “disguised” websites but also provide leads to the distributors of the most prolific commercial child sexual abuse websites identified as part of the IWF’s website brands project. It is hoped that the information set out in this briefing paper may be of assistance to law enforcement, industry stakeholders and the European Financial Coalition in disrupting and investigating the activities of individuals attempting to profit from the distribution of child sexual abuse material online.

For further information please contact the Internet Watch Foundation

(t: +44 (0)1223 203030 / e: sarah@iwf.org.uk