



Agenda item 14

Review of Usenet activity

Purpose

This paper has been prepared as a result of concerns expressed that the reporting of CAIs (Child Abuse Images) posted to newsgroups has led to an increase in notice and takedowns since the introduction of the BT Cleanfeed system in September 2004.

Executive summary

- There has been an increase in the number of 'takedowns' of potentially illegal child abuse images posted to seventy five (75) newsgroups not previously identified as failing the 'regularity' or 'names' test.
- Our opinion is that this increase has been caused by a concerted 'spam' campaign advertising nine PPV (Pay-per-view) websites that when traced contained none or lower level CAIs (Child Abuse Images).
- Only two of the nine websites advertised on the images posted was 'live' and contained actionable content.
- Apart from four (4) newsgroups which are never associated with adult content the spamming trend has been directed to seventy one (71) newsgroups linked to adult content during the September 04 to March 05 period.
- We do not believe there is a correlation between the BT Cleanfeed initiative and the increase in newsgroup 'takedowns'.
- We need to be alert to the possibility of a displacement from paedophilic newsgroups to non paedophilic newsgroups due to the IWF newsgroup 'regularity' policy.
- We will review the newsgroup 'regularity' policy to ensure that this trend does not lead to the automatic listing of otherwise legitimate newsgroups.

Viewpoint

This spam campaign could be due to a number of reasons such as:

- A. A malicious attempt to discredit usually legitimate newsgroups whereby they may fail the IWF 'regularity' test and therefore be removed from circulation by UK ISPs in accordance with IWF newsgroup policies
- B. A 'smear campaign' to discredit otherwise legitimate adult websites by posting abusive images of children to adult newsgroups stamped with the URL of an adult website (Joe Job)
- C. Ignorance on the part of the spammer as to the protocols of posting such content to non paedophilic type newsgroups
- D. An effort on the part of the spammers to tempt new clients to child abuse websites by posting to adult newsgroups



1. Introduction

At their meeting on 25 January 2005 Board asked the executive to investigate the recent increase in the number of take down notices issued for CAIs (Child Abuse Images) found in newsgroups, the intimation being that displacement was occurring because of the BT 'Cleanfeed' project.

In September 2004 BT introduced a filtering service using a database supplied by the Internet Watch Foundation. This filtering service known as Cleanfeed, filters URLs matching the list supplied by the IWF so that BT customers are not inadvertently exposed to child abuse images.

2. IWF Newsgroup policy

In November 2001 the IWF Board adopted a policy of recommending UK ISPs not to host newsgroups, which regularly contain indecent images of children. "Regularly" was defined at the February 2002 Board as:

Finding an average of at least 1% of images viewed to be illegal and additionally applying a further test whereby in each of six consecutive monitoring rounds finding any illegal content would lead to immediate listing of the group.

The IWF Hotline team has a systematic process for monitoring the content of newsgroups and for notifying ISPs of those groups where the illegal content has climbed above the approved threshold. The threshold level has been validated by DataTalk Ltd, independent specialists in statistical analysis.

3. Have CAIs increased in newsgroups since Cleanfeed was implemented?

From examination of the statistics below we can see there was a sudden increase in the number of newsgroup reports containing CAIs in September 2004. Following that 'spike' normality resumed through October to December but there was another 'spike', this time over two months in January and February 2005

If they have increased, WHY?

There are many possible reasons some of which have been listed below:

- i. 100% of the newsgroups where actionable content has been posted relate to a concerted spam campaign (across newsgroups that have not previously been associated with paedophilia e.g. Dr Who, aviation, diva and auto groups etc) to promote specific PPV (Pay-per-view) URLs originally hosted in the USA but more recently Russia. They tended to contain either none or lower level CAIs. This may be due to a malicious campaign to discredit these and legitimate adult content sites by a campaigner/competitor (also known as a 'Joe Job' see http://searchcio.techtarget.com/sDefinition/0,,sid19_gci917469,00.html)
- ii. A general increase has been seen across Europe as well as the UK. At a recent INHOPE meeting (Amsterdam Jan, 2005) the question was raised as to whether Newsgroup reporting had increased. A majority said yes. However, they did not give specific reasons for the increase or whether the reports have been coming from the same reporter as the UK or for the same reasons (e.g. spam)

- iii. Vigilante behaviour. We have encountered a disproportionate number of actioned reports being received from two or three vigilante style reporters who pass on an extremely large number of reports.
- iv. There has also been a large increase of reports from people other than the known 'vigilantes' or anonymous reporters due to the spam being targeted at newsgroups not associated with CAI content and the regular users not expecting to find such content. (19% of reports are from named members of the public and 40% from anonymous reports)
- v. An ability to bypass traditional anti-spam software associated with postings to newsgroups. (see appendix for explanation of methods used)
- vi. 12% of actioned reports have been initiated internally by Hotline staff from investigating cross-posting leads supplied by members of the public.

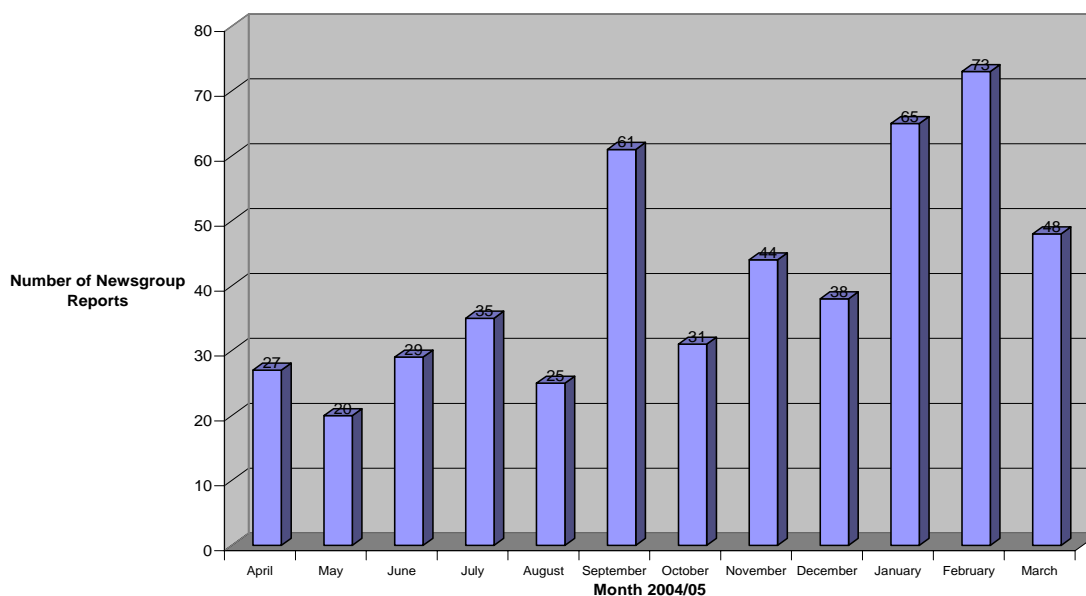


Figure 1. Monthly newsgroup reports (1/4/04 to 28/2/05)

Conclusion

With the knowledge of how spammers act (see appendix) and the surge in newsgroup reporting in just three random months we can conclude at this stage that there is no reliable evidence that the increase is due in whole or in part to the implementation of BT's Cleanfeed system.

We will review the newsgroup 'regularity' policy to ensure that this trend does not lead to the automatic listing of otherwise legitimate newsgroups and present our findings to Funding Council and Board at their July 2005 meetings.



Referenced URLs

<http://hushmail.com/about-how?PHPSESSID=95878bd12ac282477736e1026b99c779>

<http://www.anonymizer.com/anonymizer2005/1.5/>

<http://mentalhealth.about.com/library/weekly/aa081197.htm>

<http://www.iwf.org.uk>

<http://www.emailemailer.com/>

http://www.theregister.co.uk/2005/02/07/spamhaus_mci/

<http://boardsmith.netfirms.com/cgi-bin/boards/technoboard6/techno.pl>

<http://www.send-safe.com>

<http://www.mailinglistmaster.com/>

<http://hushmail.com/about-how?PHPSESSID=95878bd12ac282477736e1026b99c779>

<https://mixmaster.autistici.org/cgi-bin/mixemail-user.cgi>

<http://www.softwarevault.com/Newsreaders/Bulk-News-2002.xml>



APPENDIX

I. The Problem of Anonymous Spam/Posting

A major problem with posters of SPAM is the anonymity that posters can hide behind by using forged newsgroup headers. This makes it increasingly difficult to report an accurate point of injection for the posting in question and lead to reporting of numerous websites as a result.

Some example methods used to gain anonymity when bulk posting are shown below:

- i. Bulk Newsgroups Posting software such as "BulkNews 2002" (<http://www.softwarevault.com/Newsreaders/Bulk-News-2002.xml>) which enables you to Bulk Post to over 2000 newsgroups an hour, supports file attachments and text / HTML message format. Used in conjunction with an anonymous proxy server.
- ii. Anonymous remailers are available (e.g. <https://mixmaster.autistici.org/cgi-bin/mixemail-user.cgi>) that can be used to forward mail, however for spam postings the favourite method is to find an open mail relay server or an open/public anonymous proxy server. More information can be found at <http://hushmail.com/about-how?PHPSESSID=95878bd12ac282477736e1026b99c779>
- iii. Bulk Posting/Mailing packages such as Stealthmail Master. (<http://www.mailinglistmaster.com/>) or Send-Safe (<http://www.send-safe.com>) and direct via a remailer (see above).
- iv. Anonymous proxy servers (<http://boardsmith.netfirms.com/cgi-bin/boards/technoboard6/techno.pl>).

II. A further spam problem: (bypassing spam filters)

It is possible to bypass basic anti-spam filters such as IP address blacklists by using compromised/trojaned machines (proxies in spammer parlance or machines running Trojan software maliciously installed) - instead of open mail relays or unscrupulous hosts. The latest version of Send-Safe allows spammers to use hijacked proxies to send the spam out via the upstream ISP's main mail server, instead of from an infected machine itself. (see

http://www.theregister.co.uk/2005/02/07/spamhaus_mci/)

Spammers will include a link to a URL (website) within the spam for the 'spammed user' to click on to access. This will enable the spammer to log information regarding who is accessing the site via the spam sent (IP address, browser used etc) and a date/time stamp to review the success of the spam campaign.

Another major problem when tracking the injection point of the spam is that nearly all the headers of the postings being reported are forged. As with the previously mentioned problem, the forging of headers is relatively simple using some of the 'over the counter' products available for bulk mailing/posting (e.g. <http://www.emilemail.com/>)



III. Usenet headers and recognising forgeries

One of the problems associated with tracing usenet posters is that of forged or spoofed headers. We can identify the starting by tracing to the last known legitimate ISP contained in the posting header. To help understand how usenet headers are deciphered we will look at an example of a usenet posting header:

EXAMPLE

Path:

nnp3.clara.net!mephistopheles.news.clara.net!news.clara.net!newsfeed.icl.net!newsfeed.fjserv.net!newspeer00.lnd.ops.eu.uu.net!newspost00.lnd.ops.eu.uu.net!emea.uu.net!read.news.uk.uu.net!not-for-mail

From: "Mark Green" <markgreene67@hotmail.com>

Newsgroups: alt.test

Subject: Test for the 11th of June

Date: Fri, 6 Jun 2003 10:39:49 +0100

X-Priority: 3

X-MSMail-Priority: Normal

X-Newsreader: Microsoft Outlook Express 6.00.2800.1158

X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165

Lines: 5

Message-ID: <3ee061b5\$0\$10622\$4d4eb98e@read.news.uk.uu.net>

NNTP-Posting-Host: 193.129.101.51

X-Trace: 1054892469 read.news.uk.uu.net 10622 193.129.101.51

X-Complaints-To: abuse@uk.uu.net

Xref: mephistopheles.news.clara.net alt.test:2267961

From looking at the example above we will firstly look at the 'Path' . This "should" tell us which ISP the post was injected from. However, it is possible to preload part of this path so all we can actually tell is that it was injected at some point along the way.

Next we will look at the rest of the fields:

From: "Mark Green" markgreene67@hotmail.com

Easily faked, forged or plain From: headers are often found in either spam, junk or deliberate flames/Joe Jobs.

Newsgroups: alt.test

Only tells us which newsgroup it was posted to.

Subject: Test for the 11th of June

Date: Fri, 6 Jun 2003 10:39:49 +0100

Doesn't give us anything other than when the article was posted - you do occasionally find that the Organization: line has been filled in with something meaningful - like a company name - and then a search on Google or one of the Search Engines might bring up a Company name - treat with suspicion though - it may be faked.

Message-ID: <3ee061b5\$0\$10622\$4d4eb98e@read.news.uk.uu.net>

This should usually tell us which ISP the article was injected from. It can be faked but often shows the real ISP. If there is more than one, it means the ISP or software



automatically adds it and the poster has tried to disguise themselves

NNTP-Posting-Host: 193.129.101.51

Usually shows the host or dialup that the post was made through and is very often added by the ISP and it will then show the dialup that the post was injected through. Can be used by ISPs to then trace who posted an article.

X-Trace: 1054892469 read.news.uk.uu.net 10622 193.129.101.51

X-Trace is added automatically by a lot of news servers to help track down fake posts and spam. If present it is a good indication of the real ISP involved

X-Complaints-To: abuse@uk.uu.net

Many ISPs add this automatically when news is injected through their servers. If present then is usually a very good indication of whom to complain to.

Xref: mephistopheles.news.clara.net alt.test:2267961

All this tells us is that on my news server, this post received the article numbers that are quoted after the newsgroups. No help to anyone

From looking at the example of the usenet posting above and what each section tells us we can conclude that the X-Trace and X-Complaints-To are the best indications of the ISP that the message was injected via

NOTE

Although we can find the 'point of injection' ISP this does not guarantee that the user who posted the message is a customer of that ISP. The reason for this is due to anonymous or forged postings as outlined in Appendix I. In light of these problems it is only possible to inform the last known accurate 'point-of-injection' ISP so that they can initiate a trace through their network

IV Advertised URL's in recent usenet spam campaign

Below is a table of the URL's that are being advertised as part of the recent spam usenet campaign. From looking at the table below from left to right we can see the URL that is being advertised, the original date that the URL was reported the content, country and action taken (showing the hotline that the URL was reported to). The final four columns show the date the URL was reviewed the content, country of origin and action taken.

From the table below we can see that the content being advertised since review has in general moved predominantly to Russia from the US and that not all content is actionable.



Table 1. Advertised URL's in recent campaign.

	Date	Content	Country	Action	Review Date	Content	Country	Action
	16/01/2005	Adult Pornography	US	Cybertipline	31/03/2005	Adult Pornography	US	No
	16/01/2005	Adult Pornography	CN	No	31/03/2005	Adult Pornography	RU	No
	16/01/2005	Adult Pornography	US	Cybertipline	31/03/2005	Adult Pornography	US	No
	16/01/2005	Adult Pornography	US	Cybertipline	31/03/2005	Adult Pornography	US	No
	16/01/2005	Adult Pornography	RU	No	31/03/2005	Child Abuse Image	RU	NCIS
	16/01/2005	Adult Pornography	US	Cybertipline	31/03/2005	Site down	RU	No
	16/01/2005	Site down		No	31/03/2005	Site down		No
	07/03/2005	Child Abuse Image Level 1	RU	NCIS	31/03/2005	Child Abuse Image Level 1	RU	No
	07/03/2005	Child Abuse Image Level 1	RU	NCIS	31/03/2005	Child Abuse Image Level 1	RU	No