

Re: I think I am being attacked – Can you help?

Re: I think I am being attacked – Can you help?

Source: <http://linux.derkeiler.com/Newsgroups/linux.redhat/2008-04/msg00003.html>

- *From:* "Jim G" <jgrago@xxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 2 Apr 2008 20:42:45 -0400
-

"Johnny Rebel" <rebelATT@xxxxxxxxxxxxx> wrote in message
[news:8cfff\\$47f4104b\\$d1d97aaa\\$6974@xxxxxxxxxxxxx](mailto:news:8cfff$47f4104b$d1d97aaa$6974@xxxxxxxxxxxxx)

Jim G wrote:

Sorry if this is off topic. Not sure where to post. I am running a fedora core 4 server and over the past few months I have noticed a lot of bogus traffic hitting my servers. Infact so much so that at any given time there are from 800 to 1000 connections to any one of my servers at a time with the stuff you see below. All of the hits come from Macintosh computers, they are all calling this `/?32175, /?536235, /?2523754` and another that is not listed here is `/f=*` The `/?xxxxx` is from an affiliate program that was running on my server, but I know for a fact that this is bogus traffic because the accounts that these are related to are closed and the affiliate program is no longer running.

Listed below all this is another sort of attack, coming from youtube. (Below this snippet).

```
77.54.169.33 -- [02/Apr/2008:15:49:47 -0500] "GET /?32175 HTTP/1.1"
302 - "-" "Mozilla/5.0 (Macintosh; UP6; PPC Mac OS X; en-US)
AppleWebKit/8I1.3 (KHTML, like Geco, Safari) OmniWeb/vY42.H8"
189.46.128.138 -- [02/Apr/2008:15:49:47 -0500] "GET /?32175
HTTP/1.1" 302 - "-" "Mozilla/5.0 (Macintosh; 841; PPC Mac OS X;
en-US) AppleWebKit/5A2.1 (KHTML, like Geco, Safari)
OmniWeb/vL33.EC"
213.203.109.223 -- [02/Apr/2008:15:49:47 -0500] "GET /?32175
HTTP/1.1" 302 - "-" "Mozilla/5.0 (Macintosh; ZTV; PPC Mac OS X;
en-US) AppleWebKit/2CG.0 (KHTML, like Geco, Safari)
OmniWeb/vR13.Q4"
89.186.129.247 -- [02/Apr/2008:15:49:47 -0500] "GET /?2460341
HTTP/1.0" 200 - "-" "Mozilla/5.0 (Macintosh; COK; PPC Mac OS X;
en-US) AppleWebKit/410.4 (KHTML, like Geco, Safari)
OmniWeb/v463.21t=C:\\WINDO\\x81"
85.59.165.254 -- [02/Apr/2008:15:49:47 -0500] "GET /?536235
HTTP/1.1" 302 - "-" "Mozilla/5.0 (Macintosh; FNY; PPC Mac OS X;
en-US) AppleWebKit/1EA.1 (KHTML, like Geco, Safari)
OmniWeb/vT36.BQ"
```

Re: I think I am being attacked – Can you help?

83.77.25.99 -- [02/Apr/2008:15:49:47 -0500] "GET /?2523754 HTTP/1.0"
302 - "-" "Mozilla/5.0 (Macintosh; MOZ; PPC Mac OS X; en-US)
AppleWebKit/160.3 (KHTML, like Geco, Safari)
OmniWeb/v872.61Java\jre1.\x81"
201.14.123.228 -- [02/Apr/2008:15:49:48 -0500] "GET /?536235
HTTP/1.1" 302 - "-" "Mozilla/5.0 (Macintosh; MRN; PPC Mac OS X;
en-US) AppleWebKit/4NZ.x (KHTML, like Geco, Safari)
OmniWeb/vZ51.2S"
121.133.157.68 -- [02/Apr/2008:15:49:48 -0500] "GET /?32175
HTTP/1.1" 302 - "-" "Mozilla/5.0 (Macintosh; KV6; PPC Mac OS X;
en-US) AppleWebKit/172.3 (KHTML, like Geco, Safari)
OmniWeb/vJ37.7H"
85.87.193.139 -- [02/Apr/2008:15:49:48 -0500] "GET /?32175 HTTP/1.1"
302 - "-" "Mozilla/5.0 (Macintosh; 5LF; PPC Mac OS X; en-US)
AppleWebKit/3QJ.7 (KHTML, like Geco, Safari) OmniWeb/v515.VB"
70.55.144.248 -- [02/Apr/2008:15:49:48 -0500] "GET /?2523754
HTTP/1.0" 302 - "-" "Mozilla/5.0 (Macintosh; JGI; PPC Mac OS X;
en-US) AppleWebKit/213.5 (KHTML, like Geco, Safari)
OmniWeb/v824.15"
217.28.149.2 -- [02/Apr/2008:15:49:48 -0500] "GET /?2523754
HTTP/1.0" 302 - "-" "Mozilla/5.0 (Macintosh; DTZ; PPC Mac OS X;
en-US) AppleWebKit/301.0 (KHTML, like Geco, Safari)
OmniWeb/v807.20"
87.217.131.213 -- [02/Apr/2008:15:49:48 -0500] "GET /?2523754
HTTP/1.0" 302 - "-" "Mozilla/5.0 (Macintosh; PJS; PPC Mac OS X;
en-US) AppleWebKit/146.5 (KHTML, like Geco, Safari)
OmniWeb/v230.68"
189.7.126.158 -- [02/Apr/2008:15:49:48 -0500] "GET /?32175 HTTP/1.1"
302 - "-" "Mozilla/5.0 (Macintosh; RMD; PPC Mac OS X; en-US)
AppleWebKit/425.0 (KHTML, like Geco, Safari) OmniWeb/vQ41.ZX"
85.141.175.51 -- [02/Apr/2008:15:49:48 -0500] "GET /?32175 HTTP/1.1"
302 - "-" "Mozilla/5.0 (Macintosh; RBV; PPC Mac OS X; en-US)
AppleWebKit/2F7.5 (KHTML, like Geco, Safari) OmniWeb/vB30.I6"
83.32.16.185 -- [02/Apr/2008:15:49:48 -0500] "GET /?2460341
HTTP/1.0" 200 - "-" "Mozilla/5.0 (Macintosh; ZYE; PPC Mac OS X;
en-US) AppleWebKit/464.2 (KHTML, like Geco, Safari)
OmniWeb/v113.43ive=C:"
86.70.188.210 -- [02/Apr/2008:15:49:48 -0500] "GET /?2523754
HTTP/1.0" 302 - "-" "Mozilla/5.0 (Macintosh; APH; PPC Mac OS X;
en-US) AppleWebKit/427.2 (KHTML, like Geco, Safari)
OmniWeb/v420.87ive=C:"
41.232.217.206 -- [02/Apr/2008:15:49:48 -0500] "GET /?2523754
HTTP/1.0" 302 - "-" "Mozilla/5.0 (Macintosh; EPQ; PPC Mac OS X;
en-US) AppleWebKit/358.0 (KHTML, like Geco, Safari)
OmniWeb/v333.10"
80.54.182.184 -- [02/Apr/2008:15:49:48 -0500] "GET /?32175 HTTP/1.1"
302 - "-" "Mozilla/5.0 (Macintosh; 89P; PPC Mac OS X; en-US)
AppleWebKit/5Q4.5 (KHTML, like Geco, Safari) OmniWeb/vV12.ZO"
81.245.130.219 -- [02/Apr/2008:15:49:48 -0500] "GET /?32175
HTTP/1.1" 302 - "-" "Mozilla/5.0 (Macintosh; 5D8; PPC Mac OS X;
en-US) AppleWebKit/3JX.6 (KHTML, like Geco, Safari)

Re: I think I am being attacked – Can you help?

OmniWeb/vZ30.9E"
75.145.164.201 -- [02/Apr/2008:15:49:48 -0500] "GET /?2460341
HTTP/1.0" 200 - "-" "Mozilla/5.0 (Macintosh; FEY; PPC Mac OS X;
en-US) AppleWebKit/771.0 (KHTML, like Geco, Safari)
OmniWeb/v157.64ogram File\x81"
85.155.150.84 -- [02/Apr/2008:15:49:48 -0500] "GET /?32175 HTTP/1.1"
302 - "-" "Mozilla/5.0 (Macintosh; 3DK; PPC Mac OS X; en-US)
AppleWebKit/11G.3 (KHTML, like Geco, Safari) OmniWeb/vG71.QI"
87.219.102.226 -- [02/Apr/2008:15:49:48 -0500] "GET /?32175
HTTP/1.1" 302 - "-" "Mozilla/5.0 (Macintosh; YFS; PPC Mac OS X;
en-US) AppleWebKit/2E0.4 (KHTML, like Geco, Safari)
OmniWeb/vE66.LU"
79.9.196.135 -- [02/Apr/2008:15:49:49 -0500] "GET /?32175 HTTP/1.1"
302 - "-" "Mozilla/5.0 (Macintosh; D90; PPC Mac OS X; en-US)
AppleWebKit/2Q5.0 (KHTML, like Geco, Safari) OmniWeb/vY14.GG"
82.156.95.90 -- [02/Apr/2008:15:49:49 -0500] "GET /?2523754
HTTP/1.0" 302 - "-" "Mozilla/5.0 (Macintosh; INN; PPC Mac OS X;
en-US) AppleWebKit/656.6 (KHTML, like Geco, Safari)
OmniWeb/v500.56"
84.228.117.107 -- [02/Apr/2008:15:49:49 -0500] "GET /?32175
HTTP/1.1" 302 - "-" "Mozilla/5.0 (Macintosh; 3PY; PPC Mac OS X;
en-US) AppleWebKit/3FE.4 (KHTML, like Geco, Safari)
OmniWeb/vI12.OU"
80.236.91.61 -- [02/Apr/2008:15:49:49 -0500] "GET /?2523754
HTTP/1.0" 302 - "-" "Mozilla/5.0 (Macintosh; SFU; PPC Mac OS X;
en-US) AppleWebKit/813.2 (KHTML, like Geco, Safari)
OmniWeb/v137.52:\\Program \x81"
89.3.91.218 -- [02/Apr/2008:15:49:49 -0500] "GET /?2523754 HTTP/1.0"
302 - "-" "Mozilla/5.0 (Macintosh; UHT; PPC Mac OS X; en-US)
AppleWebKit/338.0 (KHTML, like Geco, Safari) OmniWeb/v871.10ve=C:"
201.18.37.162 -- [02/Apr/2008:15:49:49 -0500] "GET /?32175 HTTP/1.0"
302 - "-" "Mozilla/5.0 (Macintosh; TAY; PPC Mac OS X; en-US)
AppleWebKit/7W5.3 (KHTML, like Geco, Safari) OmniWeb/vU20.KW"
200.8.110.143 -- [02/Apr/2008:15:49:49 -0500] "GET /?32175 HTTP/1.1"
302 - "-" "Mozilla/5.0 (Macintosh; 4C2; PPC Mac OS X; en-US)
AppleWebKit/8NC.0 (KHTML, like Geco, Safari) OmniWeb/vP05.9V"
80.20.99.250 -- [02/Apr/2008:15:49:49 -0500] "GET /?2460341
HTTP/1.0" 200 - "-" "Mozilla/5.0 (Macintosh; TQN; PPC Mac OS X;
en-US) AppleWebKit/177.1 (KHTML, like Geco, Safari)
OmniWeb/v467.13"

From Youtube

```
[root@host5 httpd]# grep "youtube" access_log  
89.42.144.9 -- [02/Apr/2008:15:49:50 -0500] "GET /?f=* HTTP/1.1" 302  
- "http://www.youtube.com/watch?v=ZlXFjyP\_Cck&feature=related  
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"  
88.253.96.206 -- [02/Apr/2008:15:50:07 -0500] "GET /?f=* HTTP/1.1"  
302 - "http://www.youtube.com/watch?v=oYqN4o9Xvxg&feature=related  
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; FunWebProducts)"
```

Re: I think I am being attacked – Can you help?

196.206.214.178 -- [02/Apr/2008:15:50:11 -0500] "GET /?f=* HTTP/1.1" 302 - "http://www.youtube.com/watch?v=PKLFfVMqe-I "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
78.168.37.42 -- [02/Apr/2008:15:50:57 -0500] "GET /?f=* HTTP/1.1" 302 - "http://www.youtube.com "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
78.168.37.42 -- [02/Apr/2008:15:50:58 -0500] "GET /?f=* HTTP/1.1" 302 - "http://www.youtube.com "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
78.168.37.42 -- [02/Apr/2008:15:51:11 -0500] "GET /?f=* HTTP/1.1" 302 - "http://www.youtube.com/results?search_query=besyo&search_type="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
78.168.37.42 -- [02/Apr/2008:15:51:12 -0500] "GET /?f=* HTTP/1.1" 302 - "http://www.youtube.com/results?search_query=besyo&search_type="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
78.168.37.42 -- [02/Apr/2008:15:51:58 -0500] "GET /?f=* HTTP/1.1" 302 - "http://www.youtube.com/results?search_query=besyo&page=2 "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
78.168.37.42 -- [02/Apr/2008:15:51:58 -0500] "GET /?f=* HTTP/1.1" 302 - "http://www.youtube.com/results?search_query=besyo&page=2 "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
78.168.37.42 -- [02/Apr/2008:15:52:28 -0500] "GET /?f=* HTTP/1.1" 302 - "http://www.youtube.com/results?search_query=besyo&page=3 "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
78.168.37.42 -- [02/Apr/2008:15:52:29 -0500] "GET /?f=* HTTP/1.1" 302 - "http://www.youtube.com/results?search_query=besyo&page=3 "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
78.168.37.42 -- [02/Apr/2008:15:53:08 -0500] "GET /?f=* HTTP/1.1" 302 - "http://www.youtube.com/results?search_query=besyo&page=4 "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
78.168.37.42 -- [02/Apr/2008:15:53:44 -0500] "GET /?f=* HTTP/1.1" 302 - "http://www.youtube.com/results?search_query=besyo&page=5 "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
78.168.37.42 -- [02/Apr/2008:15:54:14 -0500] "GET /?f=* HTTP/1.1" 302 - "http://www.youtube.com/results?search_query=besyo&page=6 "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
78.168.37.42 -- [02/Apr/2008:15:54:43 -0500] "GET /?f=* HTTP/1.1" 302 - "http://www.youtube.com/results?search_query=besyo&page=7 "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
78.168.37.42 -- [02/Apr/2008:15:55:16 -0500] "GET /?f=* HTTP/1.1" 302 - "http://www.youtube.com/results?search_query=besyo&page=8 "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
196.206.214.178 -- [02/Apr/2008:15:55:31 -0500] "GET /?f=* HTTP/1.1" 302 -
"http://www.youtube.com/results?search_query=warda+3la+warda&search_type="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
78.168.37.42 -- [02/Apr/2008:15:55:38 -0500] "GET /?f=* HTTP/1.1" 302 - "http://www.youtube.com/results?search_query=ctl&search_type="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
78.168.37.42 -- [02/Apr/2008:15:55:55 -0500] "GET /?f=* HTTP/1.1" 302
=

Re: I think I am being attacked – Can you help?

Re: I think I am being attacked – Can you help?

"http://www.youtube.com/results?search_query=kol+bast%C4%B1&search_type=Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
78.168.37.42 -- [02/Apr/2008:15:56:02 -0500] "GET /?f=* HTTP/1.1" 302
-- "http://www.youtube.com/watch?v=yVt6rJIEueY "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1; SV1)"
196.206.214.178 -- [02/Apr/2008:15:56:03 -0500] "GET /?f=* HTTP/1.1"
302 -- "http://www.youtube.com/watch?v=wFPCa9NgNy8 "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1)"
67.139.245.131 -- [02/Apr/2008:15:56:04 -0500] "GET /?f=r HTTP/1.0"
302 -- "http://www.youtube.com/watch?feature=related&v=hIE4swcmEDY
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
67.139.245.131 -- [02/Apr/2008:15:56:05 -0500] "GET
/stormpay/user/user_auctions.php HTTP/1.0" 200 33524
"http://www.youtube.com/watch?feature=related&v=hIE4swcmEDY
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
196.206.214.178 -- [02/Apr/2008:15:56:22 -0500] "GET /?f=* HTTP/1.1"
302 -- "http://www.youtube.com/watch?v=Wzv -AjXPDY&feature=related
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
69.250.228.122 -- [02/Apr/2008:15:56:31 -0500] "GET /?f=* HTTP/1.1"
302 -- "http://youtube.com/watch?v=VbhsYC4gKy4 "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1)"
69.250.228.122 -- [02/Apr/2008:15:56:32 -0500] "GET /?f=* HTTP/1.1"
302 -- "http://youtube.com/watch?v=VbhsYC4gKy4 "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1)"

Yesterdays log file shows over 13.000 youtube entries alone.

```
[root@host5 httpd]# grep "youtube" access_log.1 | wc  
13787 284556 2904200
```

Over 1 million hits yesterday on the expression "Macintosh"

```
[root@host5 httpd]# grep "Macintosh" access_log.1 | wc  
1516665 37654811 297731520
```

This is on just one server, I have 3 that are currently online.

Now I have attempted to contact youtube, which as you know is nearly impossible. I have added some code to my page to try to stop these attacks which basically says if this expression comes in, redirect to localhost.

```
$flood_queries = array(  
'f=*',  
'2523754',  
'536235',  
'32175'  
);  
if (!empty($QUERY_STRING)) {  
foreach ($flood_queries as $flood) {  
if (stripos($QUERY_STRING,$flood)!==false) {  
header('Expires: Mon, 26 Jul 1997 05:00:00 GMT');
```

Re: I think I am being attacked – Can you help?

```
header('Last-Modified: ' . gmdate('D, d M Y H:i:s') . ' GMT');  
header('Cache-Control: must-revalidate, post-check=0, pre-check=0');  
header('Location: http://127.0.0.1/');  
die();
```

But this has not helped in any way. These hits seem to be increasing. It seems that something or someone is embedding a GET request in the youtube flv file that is created? Is that possible? Can I turn up the logging in apache to see if it shows me anything else? (Although I dont want to slow it down anymore than what it already is).

If you have any idea on what this is or how to stop it I would appreciate it.

Thanks

Jim

How does this differ from your "normal" traffic? Are you being slash dot'd? There are a few ways to block these sorts of things – one would be tcpd (if applicable – but probably/hopefully not) and the other is iptables. iptables is how I do it, by either a whole-encompassing rule to limit hits, or by specifically targeting excessive IP's/IP ranges. There are many scripts on the web for this kind of thing. The better ones basically figure out what is not normal and block that IP for a configured time. They then undo the entry. Search around and you will find.

JR.

--

Bill will have to take Linux from my cold, dead flippers.

-Tux.

Well I did try to block all of the ip's. The first time around it grabbed 3700 ip's. An hour later it grabbed some 500 more. I dont think that Iptables is the solution (Imho). Too many ip's will cause the server to slow and I cannot have that.

Now I am starting to see some hits from Orkut (googles social networking site).

```
200.101.102.50 -- [02/Apr/2008:19:34:46 -0500] "GET /?f=* HTTP/1.1" 302 -  
"http://www.orkut.com/AlbumZoom.aspx?uid=11082738752248165644&pid=1204392452629&aid=1199816159"  
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"  
200.101.102.50 -- [02/Apr/2008:19:34:47 -0500] "GET /?f=* HTTP/1.1" 302 -  
"http://www.orkut.com/AlbumZoom.aspx?uid=11082738752248165644&pid=1204392452629&aid=1199816159"  
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"  
200.6.107.166 -- [02/Apr/2008:19:34:47 -0500] "GET /?32175 HTTP/1.1" 302 - "-" "Mozilla/5.0  
(Macintosh; HF1; PPC Mac OS X; en-US) AppleWebKit/51Z.5 (KHTML, like Geco, Safari)  
OmniWeb/v852.OO"
```

Re: I think I am being attacked – Can you help?

Re: I think I am being attacked – Can you help?

200.101.102.50 -- [02/Apr/2008:19:34:47 -0500] "GET /?f=* HTTP/1.1" 302 -
"http://www.orkut.com/AlbumZoom.aspx?uid=11082738752248165644&pid=1204392452629&aid=1199816159
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"

I am not sure if I am being slash dot'd (Infact not even sure what that means). I have tried using mod rewrite rules in apache to stop this (no luck and I commented it out).

```
# <IfModule mod_rewrite.c>  
#RewriteEngine on  
#RewriteCond %{QUERY_STRING} ^32175$  
#RewriteRule ^/$ /tmp/blank.html [L]  
#RewriteRule ^/$ /dev/null [L]  
# </IfModule>  
# RewriteCond %{HTTP_USER_AGENT} ^Mozilla/5.0 (Macintosh;  
# RewriteRule ^/.* http://%{REMOTE_ADDR}/ [L,E=nolog:1]
```

Jim

^