

# FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 09/22/2008

To: Los Angeles  
FBIHQ

CIU

From: Los Angeles  
CY-2

Contact: [REDACTED]

b6  
b7C

Approved By: [REDACTED] DA

Drafted By: [REDACTED] bs SS

Case ID #: 288A-LA (Pending) - 251746 - 1

Title: UNSUB(S);  
VICTIM - BILLOREILLY.COM

Synopsis: Request to open and assign the captioned matter to  
[REDACTED]

Details:

## SUMMARY OF EVENTS

On September 19, 2008, Bill O'Reilly's website, [www.billoreilly.com](http://www.billoreilly.com) was compromised. [REDACTED] is the [REDACTED] for the site, and believes the intruder was able to access an administrative page that is normally under password protection. The intruders may have found the page by using a dictionary style attack on the websites administrative area, and found one page that was outside of the protected area. This page happened to display new users who signed up within the last five days. The page included email addresses and passwords and physical addresses for 205 "premium" members. This information was posted on Ebaumsworld.com, and is now in the public domain. b6 b7C

[REDACTED] has informed these customers of the intrusion, and refunded subscription costs. Losses from refunds given are approximately \$10,000.

At least two individuals from the 205 have reported fraud on their financial accounts due to the fact that the passwords they used were used for other sites such as Paypal, eBay, and their banking website. In speaking to one victim, she has seen approximately \$400 in fraudulent charges thus far, all of which the banks reversed. Additionally, someone has locked her

9/22/08  
O+A  
SA  
[REDACTED]  
b6  
b7C

To: Los Angeles From: Los Angeles  
Re: 288A-LA , 09/22/2008

out of her Facebook account, stating on the Facebook page that this was in retaliation for O'Reilly's comments regarding Sarah Palin's email account being hacked.

On September 20, and 21, the website suffered a Distributed Denial of Service attack (DDOS) which at it's apex was flooding the site with 1.5GB/s.

Preservation letters have been sent to relevant Internet service providers and Facebook.

Writer requests that captioned matter be opened.

♦♦

266bs01.08

# FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 10/27/2008

To: Los Angeles

Attn: SSA [REDACTED]

From: Los Angeles

Squad CY-2

Contact: SA [REDACTED]

b6  
b7C

Approved By: [REDACTED] *BSX*

Drafted By: [REDACTED]

:bs *BS*

Case ID #: 288A-LA-251746 (Pending) *-5*

Title: UNSUB(S);  
VICTIM - BILLOREILLY.COM

b6  
b7C

Synopsis: Request that captioned matter be closed.

Details: On October 24, 2008, Assistant United States Attorney, [REDACTED] was advised of the closing of the captioned matter. It was determined that the web page compromising several identities was in unprotected web space. The Internet Protocol (IP) address which first discovered this compromise was discovered to belong to a proxy website. The use of this proxy was traced back to the use of another proxy service, Vtunnel. VTunnel did not have IP address logs for the date and time of the incident. The placement of the identities in non-protected web space was an oversight.

In regards to a Distributed Denial of Service attack after the intrusion, the attack failed and was not able to bring the website down. The top three offending IP addresses were investigated. Two were outside the United States. The one that was in the United States belonged to [REDACTED] a website hosting service. [REDACTED] was not able to furnish any information. No monetary damages have been reported to the writer.

b6  
b7C

The [REDACTED] Billoreilly.com, [REDACTED] [REDACTED], has been notified of the closing of the case as it pertains to the Federal Bureau of Investigation.

b6  
b7C

In light of these facts, the writer recommends that captioned matter be closed. There is no 1B evidence associated with captioned matter.

♦♦

301bs 01.08

*a*

- 1 -

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/25/2008

[redacted] telephone number [redacted] b6 b7C  
[redacted] were interviewed at their place  
of employment, Nox Solutions 1642 Westwood Boulevard Suite 202, Los  
Angeles, California. Also present on speaker phone was [redacted]  
[redacted] of Billloreilly.com, telephone number [redacted]  
[redacted] After being  
advised of the identity of the interviewing agents and the nature  
of the interview, [redacted] provided the following information:

Approximately 200 registered users of Billloreilly.com's  
emails, passwords, and physical addresses were compromised on  
September 19, 2008. The users effected were refunded their  
subscription costs and offered a free year on top of what they had  
already paid for. The cost of this was approximately \$10,000.

Three members experienced additional fraud due to their b6 b7C  
Billloreilly.com password being the same as other passwords such as  
Paypal: [redacted] and [redacted] b6 b7C

The intrusion was first publicized in a screen-shot of 20  
to 30 users on Wikileaks. Further printouts were retrieved by [redacted]  
[redacted] on 4Chan. The writer was provided the printouts as well as  
other supporting printouts discussing the intrusion on different  
websites. One 4Chan printout of comments showed a comment that  
purported to be the individual who discovered Billloreilly.com's  
flaw. A second forum page showed discussion about a distributed  
denial of service (DDOS) attack that had failed to take  
Billloreilly.com down. The image of "EFG" was associated with the  
comments. The DDOS attack began on Sunday.

Though the DDOS attack was discussed in real-time on  
4Chan, comments were left on computerworld.com and other sites that  
described the attacks in great detail and blamed Ebaum hackers for  
being responsible.

In explaining the flaw that was exploited, [redacted] b6 b7C  
described that a servlet is used to protect administrative files on  
the website. The page containing the compromised user information  
was an administrative page that tracked recent website  
registrations. However, this page was not being protected by the  
servlet. [redacted] believes this was an oversight that occurred some

Investigation on 09/23/2008 at Los Angeles

b6  
b7CFile # 288A-LA-251746 *2*

Date dictated \_\_\_\_\_

by SA [redacted]  
SA [redacted] *MMV*

2696501-08

288A-LA-251746

b6  
b7C

Continuation of FD-302 of [REDACTED], On 09/25/2008, Page 2

time ago when he was showing someone else the page without having the page under the servlet's protection.

Logs show various IP's exploring the path of the administrative section looking for pages not under the servlet's control. The IP address [REDACTED] was one IP used to scan the path, but it also was used to login to Billoreilly.com using one of the compromised accounts at 7:30 a.m.. The original account owner had just signed up at 6:30 a.m.. This account was at the top of the list. At 10:30 a.m. all effected accounts were shut down by [REDACTED]. After further research, [REDACTED] concluded [REDACTED] to be part of a botnet that got used twice.

b6  
b7C

The DDOS attack was a UDP flood sent to high port numbers that appeared to all be above 10000. The first occurrence was Sunday morning at 5000 packets a second. The second occurrence was Sunday around 8 to 9 p.m. at 800MB/s to two servers. There was no effect on outbound traffic.

Calls have been made to [REDACTED] saying they will be raped. Presumably due to their relationship with O'Reilly. Fox security and the NYPD are investigating the matter. The intrusion may have been spurned by O'Reilly's comments regarding the Sarah Palin email hacker.

b6  
b7C

- 1 -

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/24/2008

[redacted] date of birth [redacted] telephone number [redacted] was interviewed telephonically. After being advised of the identity of the interviewing agent and the nature of the interview, [redacted] provided the following information:

[redacted] email address, [redacted] physical address, and password were compromised from the BillO'Reilly.com intrusion on September 19, 2008. The email and password was an account that she shared with her husband, and was used for many other websites. One such website was Paypal.

Paypal told [redacted] that \$119 had been charged to her Paypal account. Later, another charge would occur for \$140. Both charges were reversed by Paypal as [redacted] did not authorize the purchases. The second purchase was for penile enlargement.

[redacted] noticed that several of the purchases were sex-related in order to embarrass [redacted]. Order confirmations were routinely forwarded to her entire contact list to include her [redacted]. Other sites from which purchases were made include eBay, Amazon, and a flower company. [redacted] could not tell where the items were being shipped to. One email that stood out to [redacted] was [redacted]. The name of this person might be [redacted] telephone number [redacted] references Bill O'Reilly in his email. [redacted] said he could get [redacted] out of her situation.

Someone used [redacted] AOL account to send email of three men performing oral. The mail purported itself to be from John McCain. [redacted] eventually was able to change the password for the account.

[redacted] Facebook account was taken over, and lewd photos of naked men were posted. A message on the page said that O'Reilly's condemnation of Sarah Palin's email hacker had resulted in his website being hacked. Along with this were the words "we do not forgive, we do not forget," a phrase that is associated with the "Anonymous," online ideology.

[redacted] has since canceled all credit cards and bank accounts associated with the password and email account.

Investigation on 09/22/2008 at Los Angeles (telephonically)

File # 288A-LA-251746-3 Date dictated \_\_\_\_\_

by SA [redacted]

2686502-08

- 1 -

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/24/2008

[redacted] Triple8 Network, Incorporated, telephone number (888)508-2656, was interviewed telephonically. After being advised of the identity of the interviewing agent and the nature of the interview, [redacted] provided the following information:

[redacted] was informed by the writer that Internet Protocol (IP) address [redacted] had performed an intrusion on a Los Angeles based company on September 19, 2008 at 6:42 a.m. Pacific Standard Time. Writer advised that if it was in the normal course of business for Triple8 to follow up with their client regarding illegal activity, that they should contact their client. Writer advised that the client may be able to provide logs which show that they were not responsible for any wrongdoing, rather a user of their service may have been at fault.

Investigation on 09/24/2008 at Los Angeles (telephonically)

File # 288A-LA-251746 - 4 Date dictated \_\_\_\_\_

by SA [redacted] BS

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

2686201.03

Monday, September 22, 2008  
11:32 AM

b6  
b7c

thru paypal  
canceled

bank acct  
master credit  
unions

4 cards  
debit / credit  
all locked  
down  
with

119\$ on paypal

facebook acct was locked out  
political comments → [redacted] on facebook

b6  
b7c

[redacted] - myspace  
(did not open)

picture of guy w/ gun

saw email as McCain 3 guys going  
over.

buy purchase for penis ext 140\$  
amazon, ebay, flowers

[redacted]  
Bill O'Reilly

b6  
b7c



Netscalero for protection -

- txt sent sampling of traffic  
outbound no effect  
inbound only effect, but N's dropped

log aug. over 10 min.

3 → 10 packets/sec → range of attack  
Does is still going on

no ws shared on same IP as BO'R.

ie. Laura Ingram

'Anon' - '

know who he is

b6  
b7C

cc Fraud



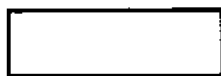
Calls to [redacted] saying they  
are going to rape her  
fox security is talking to NYPD.

Channel 11 -

YouTube - Anonymous - frightening reality

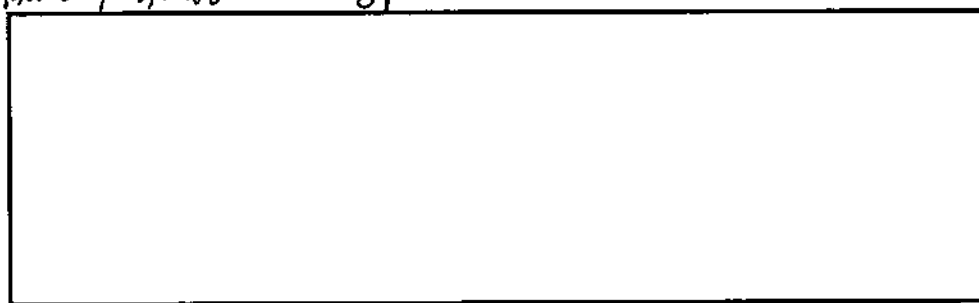
b6  
b7C

Cleveland ← NY



current postings  
lament failure spread blame

b6  
b7C



[redacted] (PT - for all) b6 b7C

- 1st compromise on 1st

had just signed up @ 6:30am

10:35am - deactivated all accounts

remainder - attempts

[redacted] IP is only IP that matches  
AOL IP/ Bot on AOL network b6 b7C

[redacted]  
scanning

Talk america

IP crossed over the 2 lists

## 2 DDOS attacks:

1) Sun Morning / minor "fail @ failing"  
5K packets / sec.

Sampling w/ IPs

high port # UDP packets

2) Sun night ~ 8pm - 9pm PT

Major ddos - pic w/ gun etc

500mb/sec to @ data center

Texas

[redacted] - gone away

Asia Pacific Netw

Hosting provider - [redacted]

b6  
b7C



to try to get him to reason  
alot of comments as well

b6  
b7C

Wikileaks - links to scr. shot

links to Zip file w/ 250 cust prof.

excel page to access

new premium member report

From inside admin path → page/secure

scan dir structure find path that wasn't  
secure

Servlet (several)

quick pg we put up w/o going thr. servlet  
just an error

by default

data for file was gener. by file itself

P- if not so eager they could have had  
a much bigger list

Can see URL req.

b6  
b7C

pg / jsp dir. structure generally

for 2th they scanned the admin dir.



- 4chan guy also a member of anon  
ebaurm-disinfo

Newswire art. had link to pg. on log  
secured path v. insecured path  
page itself now has to see if  
u r authenticated

9/23/8

Phone

Payam



Boreilly.co.,  
b6  
b7C

1yr - \$50 } refunded all / giving back 2y.  
30 d - \$5 } issued free annual memb.




\$10k loss


b6  
b7C


> 1st screen shot / 20-30 Posted - 'highly'  
Wikileaks


Printouts related to hack / 4Chan.com

Ddos Attack - weren't working  
'failed hard in failing' b6  
b7C

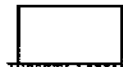
 From Bill - sent to all premium members  
thread on 4chan

yest. morning - 'efg' / pic w/ gun 

server in  trying to tk us down, but stop

\$3k in incr. bandwidth usage to fight off  
attack - 

News Articles - 1) computer world  
'anonymous'



Tuesday, September 23, 2008  
2:04 PM


b6  
b7C

If they want to remain. got there money  
back, + 1 yr if they want 50/yr  
5/m



b6  
b7C

Screen shot of 20-30. much more  
distributed on wikileaks.

 got printouts on Udon

EFG = Epic fail guy

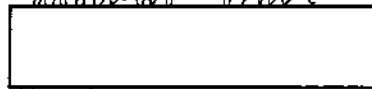
Dosser began Sunday

Usually there is a script that authenticates  
visiting.  
Got to path on 9/19

weird anonymous as user browser agent

2 paths to premium users jsp insecure/secure

P/T 7:30 am 9/19 got a login attempt from



← Asian  
public  
network  
IP

he just signed up for it 6:30

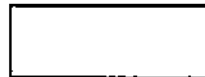
10:25 am nets shut down

b6  
b7C



crossed over between

list of login attempt



list of scan of admin site

Will call back for I.P. of actual I.P. that

got push. "premium"

high port & UDP flood on Sunday

also family is being threatened.