

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/29/2011

On December 29, 2011, Special Agent ("SA") Gabriel Andrews received by inter-office mail from the Washington Field Office a compact disk ("CD") containing chat logs between suspected members and/or affiliates of the group "Anonymous" in which one or more of the following terms were utilized:

- AESCracked
- Matthew Keys

SA Andrews analyzed the logs, and documented the following portions of the transcripts as being of interest to the Tribune media investigation (this list is non-exhaustive, and is not meant to represent the entirety of the logs, nor the entirety of the participants' activities within those logs):

#Target

Dec 08 20:53:13 <AESCracked>
if you want to attack fox news, pm me. i have a user/password for their cms

Dec 08 20:53:35 <AESCracked>
pm me for fox news password into their cms

#OperationPayback

Dec 08 20:43:15 <AESCracked>
If you're interested in hacking a FOX News site, I have a user/pass to the backend CMS for FOX40.com

Dec 08 20:44:47 <sharpie>
AESCracked: srs?

...

Dec 09 07:54:17 <AESCracked>
I've already given Ops the user/pass to several FOX websites.

Dec 09 07:54:22 <AESCracked>
The backend of their CMS.

Investigation on 12/29/2011 at Los Angeles, California

File # 288A-LA-258500-26 Date dictated Not Dictated

by SA Gabriel F. Andrews:gfa

288A-LA-258500-26

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis, On 12/29/2011, Page 2

Dec 09 08:41:24 <AESCracked>
Members of the media: I am a former journalist.

...

Dec 10 21:40:28 *
AESCracked wants us to target FOXNews.com

Dec 10 21:41:12 *
AESCracked suggests targeting FOX News

Dec 10 21:41:29 <anon73858>
never the media

Dec 10 21:41:45 <AESCracked>
FOX News is not "media"

Dec 10 21:43:58 <AESCracked>
FOX News is not media. it's "infotainment" for inbreds. I say we target them.

Dec 10 21:44:18 <mek>
AESCracked, you're correct, but people percieve them to be media, and that would be very bad for us

Dec 10 21:45:10 *
AESCracked suggests FOX News

...

Dec 11 01:56:40 <AESCracked>
No target at the moment?

...

Dec 14 02:25:11 <AESCracked>
Mission accomplished? Is Operation Payback over?

Dec 14 15:29:50 <AESCracked>
Anyone interested in defacing FOX, LA Times?

Dec 14 15:29:55 <Raphael>
no media

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis, On 12/29/2011, Page 3

Dec 14 15:29:58 <n3ot0xin>
yes AES

Dec 14 15:30:07 <rand0m>
lol ... AESCracker ... you little angry man

Dec 14 15:30:08 <AESCracked>
I have users/pass into their CMS.

...

Dec 14 16:44:37 <AESCracked>
Anonymous hackers preparing for arrests?

Dec 14 16:44:37 <AESCracked>
Are we going to be arrested?

...

Dec 19 16:10:50 <AESCracked>
Anyone want to buy an email list?

...

Dec 20 19:57:10 <AESCracked>
Adrian Lamo is gay.

Dec 20 19:57:13 <AESCracked>
Look, I know the guy personally.

Dec 20 19:57:15 <AESCracked>
...he's gay.

Dec 20 19:57:40 <blackflag>
so are you?

Dec 20 19:57:46 <AESCracked>
I'm gay, yes.

Dec 20 19:57:56 <blergh>
ha-ha!

Dec 20 19:57:57 <AESCracked>
And not as a joke either, haha.

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis, On 12/29/2011, Page 4**#internetfeds**

Dec 08 20:55:12 <Sabu>
that would be nice to get access to fox. let me know if I
can get access. I want to see if I can get further in.

Dec 08 20:56:23 <sharpie>
I asked him not to mention it in main again

Dec 08 20:56:53 <sharpie>
I was already talking to him

Dec 08 20:57:19 <sharpie>
[01:58] <AESCcracked> it takes a while to grant one
username permission to every site.

Dec 08 20:57:21 <sharpie>
[01:58] <AESCcracked> i'm doing that now.

Dec 08 20:57:19 <Sabu>
great

Dec 08 20:58:24 <Switch>
I'm talking to him too, why can't we just invite him
here?

Dec 08 20:58:24 <sharpie>
[01:59] <AESCcracked> in the meantime, these are the urls
to access their cms.

Dec 08 20:58:26 <sharpie>
[01:59] <AESCcracked>
<http://assembler.tribuneinteractive.com>

Dec 08 20:58:33 <sharpie>
okay

Dec 08 20:58:53 *
Switch invited AESCracked into the channel.

Dec 08 20:59:12 <sharpie>
oh switch already did

Dec 08 20:59:20 <AESCcracked>
i'm not a hacker.

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis, On 12/29/2011, Page 5

Dec 08 20:59:23 <AESCracked>
i'm an ex-employee

Dec 08 20:59:25 <sharpie>
[02:00] <AESCracked> that is known as
"oxygen/assembler." it is their old cms. you can publish
content, change user settings, all sortsof shit.

Dec 08 20:59:27 <sharpie>
[02:00] <AESCracked> <http://p2p.tribuneinteractive.com>

Dec 08 20:59:28 <sharpie>
[02:00] <AESCracked> that is their wysiwyg website
builder/content publisher. also controls their user-
generated content where available.

Dec 08 20:59:30 <sharpie>
yeah

Dec 08 20:59:35 <AESCracked>
finally, this is their video cms

Dec 08 20:59:40 <AESCracked>
<http://vidauth.tribune.com>

Dec 08 20:59:48 <Sabu>
hi AESCracked.

Dec 08 20:59:51 <AESCracked>
is this where i should put the superuser username and
passcode?

Dec 08 20:59:54 <AESCracked>
hi sabu

Dec 08 21:00:30 <sharpie>
<http://assembler.tribuneinteractive.com>

Dec 08 21:00:31 <sharpie>
<http://p2p.tribuneinteractive.com>

Dec 08 21:00:33 <sharpie>
<http://vidauth.tribune.com>

Dec 08 21:00:38 <sharpie>

288A-LA-258500

Continuation of FD-302 of

IRC Log Analysis

, On 12/29/2011 , Page 6

yeah AESCracked

Dec 08 21:00:44 <AESCracked>
yes, those are the three cms that this user/pass gives
access to

Dec 08 21:00:47 <AESCracked>
user: anon1234

Dec 08 21:00:50 <AESCracked>
pass: common2

Dec 08 21:01:23 <AESCracked>
go fuck some shit up!

Dec 08 21:01:29 <sharpie>
thanks very much

Dec 08 21:01:32 <sabu>
AESCracked: thank you.

Dec 08 21:01:45 <Sabu>
AESCracked: question; do you have access to their
internal servers? filesystems?

Dec 08 21:01:52 <AESCracked>
i do not.

Dec 08 21:02:10 <Sabu>
AESCracked: ok. what about email server? do they use
webmail/exchange/anything interesting?

Dec 08 21:02:26 <AESCracked>
they have microsoft exchange.

Dec 08 21:02:42 <Chronom>
AESCracked, can you paste everything here?
<http://internetfeds.prvt.org:9000/tz24eSD8Lc>

Dec 08 21:02:45 <AESCracked>
i have vpn ip addresses if that helps?

Dec 08 21:03:00 <Sabu>
AESCracked: do you have access into their vpn?

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis, On 12/29/2011, Page 7

Dec 08 21:03:05 <AESCracked>
not anymore.

Dec 08 21:03:08 <AESCracked>
ex employee remember?

Dec 08 21:03:54 <Sabu> AESCracked: understood. does not
hurt ot ask :)

Dec 08 21:04:37 <AESCracked>
i just typed in that pad link you sent me.

Dec 08 21:04:47 <AESCracked>
does the text autosave or do i need to press something to
save it?

Dec 08 21:05:02 <Sabu>
autosaves

Dec 08 21:05:26 <sharpie>
fuck

Dec 08 21:05:30 <sharpie>
we're in

Dec 08 21:05:34 <sharpie>
thanks bro

Dec 08 21:05:55 <AESCracked>
if you want the largest impact:

Dec 08 21:06:18 <AESCracked>
target the chicago tribune, the los angeles times, wpix,
klla, kcpq, ktxl, wgn-tv, antenna tv

Dec 08 21:06:39 <Kayla>
stick a big fucking Operation Payback logo on it

Dec 08 21:06:45 <AESCracked>
also, tribune wises up. they deleted a superuser account
of mine two weeks after it was created. they're not the
fastest bunch, but they're close.

Dec 08 21:06:57 <AESCracked>
oh, and any station in connectic.

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis, On 12/29/2011, Page 8

Dec 08 21:07:02 <AESCracked>
wtic, hartford courant...

Dec 08 21:07:10 <AESCracked>
those are tribune's bread and butter assets.

Dec 08 21:07:41 <AESCracked>
but if you want to make the largest impact, the ones to
target: chicago tribune, la times, ktla, ktxl, and wpix

Dec 08 21:07:50 <Chronom>
AESCracked, can you post that foxnews stuff too to the
pad?

Dec 08 21:08:08 <AESCracked>
i don't have access to foxnes.com -- they're a separate
company.

Dec 08 21:08:20 <AESCracked>
just local fox affiliates. smaller, fox-owned tv stations
and tribune newspapers in america.

Dec 08 21:08:38 <Chronom>
Sorry, I meant fox40

Dec 08 21:08:53 <AESCracked>
oh fox40 is a part of the tribune company.

Dec 08 21:09:06 <Chronom>
so those logins will be for everything?

Dec 08 21:09:27 <AESCracked>
yes

Dec 08 21:09:30 <AESCracked>
absolutely

Dec 08 21:09:31 <AESCracked>
http://en.wikipedia.org/wiki/Tribune_Broadcasting

Dec 08 21:09:37 <AESCracked>
that's a list of their stations. note the ones that say
"fox" next to them.

Dec 08 21:09:50 <Sabu>

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis, On 12/29/2011, Page 9

I am looking through these accounts. anon1234 stands out like a sore thumb. we need to blend in better amongst these other users

Dec 08 21:10:23 <AESCracked>
okay. create a fictitious name then.

Dec 08 21:10:54 <AESCracked>
if you're on the assembler site, scroll down on the left to "user preferences." click on that, then click "edit users"

Dec 08 21:11:16 <AESCracked>
when it says "find user," type "anon1234" into username then click "find"

Dec 08 21:11:19 <Sabu>
AESCracked: working on it mate. gracias :)

Dec 08 21:14:04 <AESCracked>
i'm looking through my manuals, trying to see if i can find other stuff

Dec 08 21:19:35 <Sabu>
AESCracked: we're poking around. I'm honestly looking for a way into the server.

Dec 08 21:39:23 <AESCracked>
what's the govt passwords for? what lulz will be unleashed soon? or is that for me to not know? :P

Dec 08 21:40:04 <kayla>
how di dyou know about the gov passwords?

Dec 08 21:41:29 <Sabu>
kayla: because he/she looked at the pad.

Dec 08 21:41:30 <AESCracked>
it says "govt passwords / tribune passwords"

Dec 08 21:41:59 <Chronom>
dw, the gov passwords haven't been posted ont he pad yet.

Dec 08 21:43:23 <AESCracked>
they were posted. i saw them

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis, On 12/29/2011, Page 10

Dec 08 21:43:31 <AESCracked>
what are they for?

Dec 08 21:46:06 <AESCracked>
okay i can see that was a bad question to ask.

Dec 08 21:46:19 <Switch>
what are what for?

Dec 08 21:46:30 <AESCracked>
the passwords! i want in on the fun

Dec 08 21:46:47 <kayla>
AESCracked: it is for very rainy day :D

Dec 08 21:46:52 <AESCracked>
haha

Dec 08 21:46:56 <AESCracked>
but what are they forrrrrrr?

Dec 08 21:47:28 <kayla>
Well... they are potential access to gov accounts, the
rest is your imagination

Dec 08 21:48:10 <AESCracked>
oh just potential. that's not as sexy.

Dec 08 21:48:28 <Sabu>
AESCracked: research. the same purpose the access you
gave us is for.

Dec 08 21:49:50 <AESCracked>
also, i did not give you those passwords for "research."
i want you to fuck shit up.

Dec 08 21:50:22 <Chronom>
first we have to extract as much as possible, see if we
can actually root the server

Dec 08 21:50:32 <Chronom>
if we root the server, we can extract their emails - more
lulz

Dec 08 21:50:59 <kayla>

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis , On 12/29/2011 , Page 11

are you able to upload to the server via one of those accounts?

Dec 08 21:51:10 <kayla>
or adit pages and includ php script?

Dec 08 21:51:15 <kayla>
edit*

Dec 08 21:52:01 <kayla>
stick a php command ececutiion shell on there and let me smack it with Oday :D:D

Dec 08 21:52:27 <Sabu>
well it'll have to be a jsp shell, as the backend is jsp/java.

Dec 08 21:52:43 <Chronom>
do jsp shells exist :P

Dec 08 21:52:48 <Sabu>
yes they do

Dec 08 21:52:52 <Sabu>
I got one here

Dec 08 21:53:28 <AESCracked>
http://media.trb.com is where their images and other shit is hosted.

Dec 08 21:55:27 <pellsson>
@jsp there is some hack to execute php from jsp (if php is installed that is ;))

Dec 08 21:55:33 <AESCracked>
everything on their intranet is .trb

Dec 08 21:55:35 <AESCracked>
triblink.trb

Dec 08 21:55:46 <AESCracked>
afdi.trb

Dec 08 21:55:46 <AESCracked>

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis , On 12/29/2011 , Page 12

so if you see something that ends in .trb, that's their intranet shit.

Dec 08 22:00:02 <AESCracked>
so i'm guessing you didn't see the link that said "edit web servers?"

Dec 08 22:01:52 <AESCracked>
it has dns names and doc roots and a ton of other shit.

Dec 08 22:03:08 <Sabu>
thats on the tribune cms?

Dec 08 22:03:11 <AESCracked>
yes.

Dec 08 22:03:17 <AESCracked>
go to <http://assembler.tribuneinteractive.com>

Dec 08 22:03:18 <AESCracked>
log in.

Dec 08 22:03:36 <AESCracked>
under "superuser," scroll down to "content support tables" and click "edit web servers"

Dec 08 22:03:43 <AESCracked>
..."superuser" is on the left.

Dec 08 22:03:59 <AESCracked>
sorry, to clarify...click on "superuser" then scroll down to "content support tables"

Dec 08 22:05:21 <Sabu>
nice I see that

Dec 08 22:05:23 <Sabu>
good info to have

Dec 08 22:07:08 <AESCracked>
here is a manual

Dec 08 22:07:08 <AESCracked>
<https://assembler.tribuneinteractive.com/docs/>

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis, On 12/29/2011, Page 13

Dec 08 22:07:27 <Sabu>
reading up on it

Dec 08 22:07:28 <Sabu>
niceee

Dec 08 22:10:01 <AESCracked>
just added the manual linkto the pad

Dec 08 22:14:36 <pellsson>
Sabu:whats your quest? defacing or uid0?

Dec 08 22:14:50 <Sabu>
uid0 is the name of my game

Dec 08 22:15:10 <pellsson>
mmm, the only game worth playing :)

Dec 08 22:15:23 <pellsson>
is the os known?

Dec 08 22:16:04 <Sabu>
linux box running jsp/tomcat

...

Dec 09 18:33:57 <AESCracked>
Yet another reason the Times must be demolished.

Dec 09 18:33:57 <AESCracked>
http://latimesblogs.latimes.com/the_big_picture/2010/12/wy-the-wikileaks-are-not-quite-rosa-parks.html

...

Dec 12 20:39:17 <kayla>
Now what i want to know is how this
<http://livenewswire.tumblr.com/post/2193187908/actual-passwords-have-been-redacted-government>

Dec 12 20:39:19 <kayla>
happened

Dec 12 20:39:42 <kayla>

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis, On 12/29/2011, Page 14

it was someone in here i have my ideas and i'd rather
them tell me wtf is going on

Dec 12 20:40:17 <kayla>
that txt file was only posted in here

Dec 12 20:50:01 <AESCracked>
wtf??

...

Dec 19 17:31:37 <AESCracked>
In full disclosure: I own a Mac, but I most certainly do
not own that brand of printer.

Dec 19 17:33:10 <AESCracked>
Maybe we're looking at this the wrong way.

Dec 19 17:33:19 <AESCracked>
What if someone gave PBS the link and they printed it off
a Mac using that kind of printer?

Dec 19 17:38:01 <Chronom>
has anyone from pbs news ever came to this network?

Dec 19 17:38:10 <Chronom>
i.e. in #reporters

Dec 19 17:38:13 <AESCracked>
I don't think I've seen anyone

...

Dec 20 20:01:06 <owen>
but im a USfag

Dec 20 20:01:11 <owen>
you?

Dec 20 20:01:17 <AESCracked>
I'm a USfag

Dec 20 20:01:23 <AESCracked>
West Coast represent

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis, On 12/29/2011, Page 15

Dec 20 20:01:24 *
owen perks

Dec 20 20:01:27 <owen>
oh

Dec 20 20:01:30 <owen>
midwest

Dec 20 20:02:04 <AESCracked>
Travel to where I am :D

Dec 20 20:02:18 <owen>
sweet

...

Dec 20 20:16:43 <AESCracked>
I'm somewhat cute, but not hawt.

Dec 20 20:16:53 <AESCracked>
I has golden brown hair, brown eyes...

Dec 20 20:16:57 <AESCracked>
White guy...

...

Jan 05 20:21:41 <kayla>
so you think he gonna start media dumping?

Jan 05 20:21:52 <Tred>
<Tred> okay. So you grown a conscience, fine, feel free to
do what you wish, but it's gonna be a boomerang

Jan 05 20:21:52 <Tred>
<AESCracked> Boomerangs don't always return to the
thrower.

Jan 05 20:21:52 <Tred>
<Tred> this one will

Jan 05 20:21:52 <Tred>
<Tred> you've been part of this operation

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis, On 12/29/2011, Page 16

Jan 05 20:21:53 <Tred>
<Tred> and internetfeds recently discoreved good things
for #optunisia

Jan 05 20:21:55 <Tred>
<Tred> gov stealing passowrds, now ppl know, and that's a
good thing

Jan 05 20:21:57 <Tred>
<AESCracked> I've never been part of the operation.

Jan 05 20:21:59 <Tred>
<AESCracked> Just a lurker ;)

Jan 05 20:22:01 <Tred>
<AESCracked> Nice try though.

Jan 05 20:22:03 <Tred>
<Tred> all the information you got is wrong

Jan 05 20:22:05 <Tred>
<Tred> internetfeds never hacked gawker

Jan 05 20:22:07 <Tred>
<Tred> an we don't like ppl like you lurking here without
contribue

Jan 05 20:22:09 <Tred>
<AESCracked> You think you have me all figured out :)

Jan 05 20:22:11 <Tred>
* AESCracked has quit (User has been permanently banned
from AnonOPs.net (Never forget, things can be a
boomerang.))

Jan 05 20:22:20 <Tred>
fucking idiot

Jan 05 20:23:10 <Sabu>
yeah total douch

Jan 05 20:23:12 <Sabu>
thanks tred.

Jan 05 20:23:16 <Tred>

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis . On 12/29/2011 , Page 17

:)

Jan 05 20:24:37 <Sabu>
hes online again

Jan 05 20:24:38 <kayla>
02:18 <kayla> i thought we were friends? just because you
n tflow had a tiff doesn't mean you have to be like this
thats just selfish i thought you were moe mature thn tht

Jan 05 20:24:44 <kayla>
02:18 <AESCracked> We are friends. And friends stand up
for each other. I've stood up for you a few times.

Jan 05 20:24:47 <kayla>
02:18 <AESCracked> You probably didn't know it though.

Jan 05 20:24:50 <kayla>
02:19 <AESCracked> And like I told tflow, I've been
trying to screw over one of the leaks fro about a week
now because I felt it was more important to be loyal to
you and to everyone else in that room.

Jan 05 20:24:56 <kayla>
02:21 <kayla> how do you mean you stood up for me?

Jan 05 20:24:58 <kayla>
02:22 <AESCracked> You pull off some crazy stuff. But
don't make the mistake of thinking that makes you liked
by everyone. I think some people needed to remember their
place.

Jan 05 20:25:04 <kayla>
02:24 <kayla> i dont get what you're saying?

Jan 05 20:25:07 <kayla>
02:24 <AESCracked> It doesn't matter kayla.

Jan 05 20:25:09 <kayla>
02:24 <kayla> it does because now i feel like your pissed
at me for something i have no control over

Jan 05 20:25:13 <kayla>
02:24 <kayla> and thts not fair

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis, On 12/29/2011, Page 18

Jan 05 20:25:15 <kayla>

02:25 <AESCracked> I'm not pissed at you at all.

Jan 05 20:25:18 <kayla>

02:25 <AESCracked> I'm disappointed by how the whole situation turned out.

Jan 05 20:25:20 <kayla>

02:25 <AESCracked> And I'm worried for you and for a handful of the feds because I know about shit that's going to go down and I know who is in charge of pulling the trigger.

Jan 05 20:25:26 <kayla>

02:26 <AESCracked> It disappoints me because there was a good chunk of time when I didn't fit in anywhere, and finally I fit in somewhere, even if it was among a group of renegade criminals. You guys were funny and smart and very patient even though I'm internet dumb. And then this happens and it sucks balls.

Jan 05 20:25:35 <kayla>

02:29 <kayla> what's going to go down?

Jan 05 20:25:38 <kayla>

02:59 <AESCracked> Don't worry about it. You'll know when it happens.

Jan 05 20:25:40 <kayla>

03:05 <kayla> i wont

Jan 05 20:25:43 <kayla>

lol he not know tht i been doing what i do for a long time and i've been reported to ic3 more times than i've had hot dinners

Jan 05 20:25:46 <kayla> im not so easily dox'd/v&

Jan 05 20:26:50 <garrett>
same

Jan 05 20:26:51 <garrett>
lol

Jan 05 20:26:53 <garrett>

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis, On 12/29/2011, Page 19

who is this clown

Jan 05 20:27:01 <tflow>
i genuinly believe that he could very well be the person
who leaked the government emails

Jan 05 20:27:02 <Sabu>
hes trolling

Jan 05 20:27:25 <garrett>
i dont have enough packets to throw

Jan 05 20:27:41 <tflow>
Only like 4 people ever saw that pad

Jan 05 20:27:51 <tflow>
And who else would fully report it to the media?..

Jan 05 20:28:08 <tflow>
and it kinda proves it further by the fact he's
threatening to leak more right now

Jan 05 20:28:48 <Sabu>
yup

Jan 05 20:29:08 <kayla>
meh :D

Jan 05 20:29:11 <kayla>
dramaz

Jan 05 20:29:21 <kayla>
doesn't care \:3/

Jan 05 20:29:35 <Tred>
* ***Notice -- Client connecting at
belldandy.anonops.ru:A2SCracked (A2SCracked@75-53-171-
204.lightspeed.nscrca.sbcglobal.net)

Jan 05 20:29:35 <tflow>
well the only thing I care about is if there's traitors
here

Jan 05 20:29:50 <kayla>
75-53-171-204.ightspeed.nscrca.sbcglobal.net

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis , On 12/29/2011 , Page 20

Jan 05 20:29:59 <tflow>
haha

Jan 05 20:29:59 <kl0ps>
free hugs \o/

Jan 05 20:30:00 <kayla>
that's a real ISP :D/

In the following AESCracked.txt transcript, SA Andrews converted the timestamps from Unix code to a readable format:

AESCracked.txt

12/21/10 1:32 AM UTC <AESCracked>
I has nudes! :S

12/21/10 1:32 AM UTC <owen>
i want!!

12/21/10 1:32 AM UTC <AESCracked>
ORLY? :)

12/21/10 1:32 AM UTC <owen>
anon51213@gmail.com

12/21/10 1:33 AM UTC <AESCracked>
I should set up an anon gmail.

#operationBOA

Dec 27 02:08:18 <AESCracked>
Why don't you people read the goddamn topic?!

Dec 27 02:08:23 <AESCracked>
It tells you when we're going to attack

...

Dec 27 13:45:03 <AESCracked>
Bank of America UP in West Coast

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis . On 12/29/2011 . Page 21

In the following AESCracked.txt transcript, SA Andrews converted the timestamps from Unix code to a readable format:

localhost-tflow.log

```
Jan 05 19:18:11 <tflow>
hey

Jan 05 19:18:18 <owen>
hi

Jan 05 19:18:31 <tflow>
Can you give us the IP of AESCracked?

Jan 05 19:18:38 <tflow>
He's a leaker of #internetfeds

Jan 05 19:18:42 <tflow>
He's been leaking shit

Jan 05 19:18:50 *
[AESECracked] (~AESECracked@my.vhost):AESECracked
[AESECracked] is using modes +iwrxt
[AESECracked] is connecting from *@78.129.220.46
78.129.220.46
[AESECracked] is a registered nick
[AESECracked] ?#reporter ~#raeprooom #OperationPayback
[AESECracked] vendetta.instant-panic.com :AnonOps IRC
Network
[aesecracked] End of WHOIS list.

Jan 05 19:18:53 <tflow>
A traitor all along

Jan 05 19:19:16 <owen>
i have an email addy fro him too

Jan 05 19:20:40 <owen>
dudenudeguy@gmail.com
```

288A-LA-258500

Continuation of FD-302 of IRC Log Analysis, On 12/29/2011, Page 22

SA Andrews conducted a geolocational lookup of the internet protocol ("IP") address 75.53.171.204 for the date January 6, 2011, finding it to have been assigned to SBC Internet Services in Sacramento, California, from December 1, 2010 to February 1, 2011. SA Andrews then searched connection logs for the chat transcripts referenced above, and confirmed that IP address 77.53.171.204 was used by AESCracked to connect to the IRC repeatedly between the dates of December 12, 2010 and January 5, 2011. The results of this IP search are included in the attached 1A envelope.

SA Andrews conducted a lookup of the IP address 78.129.220.46, finding it to be owned by Rapidswitch Ltd, address Clivemont Road, Maidenhead, SL6 7FW, United Kingdom, telephone number +44 (0) 1753 471 040. This IP address has been discussed previously in Serial 15 of this case file.

The CD containing the chat logs referenced above has been included in the attached 1A envelope.