## Conversation with yohoho@jabber.ccc.de at 2/16/2012 8:30:53 AM on LeonDavidson@jabber.org/jabber.org (jabber)

(8:30:56 AM) **leondavidson@jabber.org/jabber.org:** morning
(8:36:12 AM) **leondavidson@jabber.org/jabber.org:** whats good nigga
(3:29:43 PM) **The encrypted message received from yohoho@jabber.ccc.de is unreadable, as you are not currently communicating privately.**
(3:29:50 PM) **Unverified conversation with yohoho@jabber.ccc.de/ghost started.**
(3:29:51 PM) **yohoho@jabber.ccc.de:** [resent] yoyo
(3:41:28 PM) **yohoho@jabber.ccc.de:** yoyo
(3:44:57 PM) **yohoho@jabber.ccc.de:** lol @ http://twitter.com/#!/MotorSec
(4:49:09 PM) **yohoho@jabber.ccc.de:** yo
(5:22:03 PM) **yohoho@jabber.ccc.de:** yoyo
(7:04:29 PM) **yohoho@jabber.ccc.de:** yo
(7:04:30 PM) **yohoho@jabber.ccc.de:** you around ?
(7:06:53 PM) **leondavidson@jabber.org/jabber.org:** yo
(7:06:54 PM) **leondavidson@jabber.org/jabber.org:** im here
(7:06:56 PM) **leondavidson@jabber.org/jabber.org:** what up
(7:07:11 PM) **yohoho@jabber.ccc.de:** yodoing big things
(7:07:18 PM) **yohoho@jabber.ccc.de:** ok so
(7:07:23 PM) **yohoho@jabber.ccc.de:** bout to ride on these FTC losers in a few I think
(7:07:37 PM) **yohoho@jabber.ccc.de:** do you remember if you were able to crack any of these?
(7:07:41 PM) **yohoho@jabber.ccc.de:**

```
+-----+----------------+---------------------------------+---------
---------------------+------+------+-----------+-------+-----------+------------------+------------+-----------
-+------------+--------+----------+----------+---------+----------------------------+------------------------
----------------------------------------------------------------------------------------------------------+---
---------------+
| uid | name | pass | mail | mode | sort | threshold | theme | signature | signature_format | created |
access | login | status | timezone | language | picture | init | data | timezone_name |
+-----+----------------+---------------------------------+-----------------------------+------+------+-------
----+-------+-----------+------------------+------------+------------+------------+--------+----------+-------
---+---------+----------------------------+-----------------------------------------------------------------
---------------------------------------------------------------+------------------+
| 0 | | | | 0 | 0 | 0 | | | 0 | 0 | 0 | 0 | 0 | NULL | | | | NULL | |
| 1 | JGatsby | c082517d1085a83614a813a83ca4860c | julia.robinson@fleishman.com | 0 | 0 | 0 | |
| 0 | 1255369012 | 1328728099 | 1328726960 | 1 | -18000 | | | julia.robinson@fleishman.com |
a:3:{s:13:"form_build_id";s:37:"form-
d6065b4ed00c4eff6aaeba8301108779";s:18:"admin_compact_mode";b:0;s:21:"force_password_
change";i:0;} | America/New_York |
| 4 | editor | 3e6adc56a37894a45cd8bde08e0db5da | juliamarierobinson@gmail.com | 0 | 0 | 0 | | |
0 | 1266253449 | 1288813538 | 1288813538 | 1 | -18000 | | | juliamarierobinson@gmail.com |
a:2:{s:13:"form_build_id";s:37:"form-
1945f4669558fa717b3bce74baed42a9";s:21:"force_password_change";i:1;} |
America/New_York |
| 5 | kathryn | 3e6adc56a37894a45cd8bde08e0db5da | kathryn.devito@fleishman.com | 0 | 0 | 0 | |
| 0 | 1280955058 | 1281116519 | 1281026587 | 1 | -18000 | | | kathryn.devito@fleishman.com |
a:2:{s:13:"form_build_id";s:37:"form-
19d0adca2015798181b3e0c834089e1f";s:21:"force_password_change";i:1;} |
America/New_York |
| 6 | Lesley Fair | 24586b8843fa3d105424f9572c155760 | lfair@ftc.gov | 0 | 0 | 0 | | | 0 |
1281105176 | 1329409710 | 1329406343 | 1 | -18000 | | | lfair@ftc.gov |
a:2:{s:13:"form_build_id";s:37:"form-
265b731b55fee86c016f2e9214c3abf3";s:21:"force_password_change";i:1;} |
America/New_York |
| 7 | Alvaro Puig | 68fb98e6a5fe3a59ef2f85bb0b3a6cb7 | apuig@ftc.gov | 0 | 0 | 0 | | | 0 |
1281105222 | 1328735211 | 1328735204 | 1 | -18000 | | | apuig@ftc.gov |
a:2:{s:13:"form_build_id";s:37:"form-
508cba906e4763cef7a0cb60175f8790";s:21:"force_password_change";i:1;} |
America/New_York |
| 8 | Jon Morgan | 07ebbd910fef433aa47083476b5f147e | jmorgan@ftc.gov | 0 | 0 | 0 | | | 0 |
1281105242 | 1327435132 | 1327435131 | 1 | -18000 | | | jmorgan@ftc.gov |
a:2:{s:13:"form_build_id";s:37:"form-
be2a46631d6e4ec7507203f152e6d80e";s:21:"force_password_change";i:1;} |
America/New_York |
| 9 | Jessica Skretch | 93d53bb343d15752c18ddfc801038cad | jskretch@ftc.gov | 0 | 0 | 0 | | | 0 |
1281105275 | 1327426920 | 1327426920 | 1 | -18000 | | | jskretch@ftc.gov |
a:2:{s:13:"form_build_id";s:37:"form-
3d594e7658a018e2d0a75b2d76523d8a";s:21:"force_password_change";i:1;} |
America/New_York |
| 11 | Chris Hundycz | 22377565c8f3c7c7b22d027bbeb3dfdc | chundycz@ftc.gov | 0 | 0 | 0 | | | 0 |
1286821528 | 1327959413 | 1327959413 | 1 | -18000 | | | chundycz@ftc.gov |
a:2:{s:13:"form_build_id";s:37:"form-
10febba1311ead920f68aee491f7e656";s:21:"force_password_change";i:1;} |
America/New_York |
| 12 | TJ Peeler | 421469687753021f875e980ef1ad5810 | tpeeler@ftc.gov | 0 | 0 | 0 | | | 0 |
1286821550 | 1327428788 | 1327428828 | 1 | -18000 | | | tpeeler@ftc.gov |
a:2:{s:13:"form_build_id";s:37:"form-
c799e6065d0684840753958b58d09c6c";s:21:"force_password_change";i:1;} |
America/New_York |
| 13 | Carrie Gelula | 5b25b524df4f72cf06fe72d8e4a231d2 | cgelula@ftc.gov | 0 | 0 | 0 | | | 0 |
1286821578 | 1329428873 | 1329428323 | 1 | -18000 | | | cgelula@ftc.gov |
a:2:{s:13:"form_build_id";s:37:"form-
13f257ba725a2272d545c93e4caa8bda";s:21:"force_password_change";i:1;} |
America/New_York |
+-----+-----------------+---------------------------------+------------------------------+------+------+-------
----+-------+-----------+------------------+------------+------------+------------+--------+----------+-------
---+---------+-----------------------------+-------------------------------------------------------------------
---------------------------------------------------------------+------------------+
```

(7:08:02 PM) **leondavidson@jabber.org/jabber.org:** hmm I think those passwords were long/hard to crack
(7:08:06 PM) **leondavidson@jabber.org/jabber.org:** my boy hit them for a bit

```
(7:08:07 PM) yohoho@jabber.ccc.de: would have been nice to get her gmail
(7:08:10 PM) yohoho@jabber.ccc.de: yeah hrmm
(7:08:17 PM) yohoho@jabber.ccc.de: I wonder if wordpress or whatever uses some special key
(7:08:18 PM) yohoho@jabber.ccc.de: or something
(7:08:27 PM) yohoho@jabber.ccc.de: err rather this is drupal
(7:08:28 PM) yohoho@jabber.ccc.de: but anyway
(7:08:33 PM) leondavidson@jabber.org/jabber.org: possible or they're using dod standard passwords
(7:08:44 PM) leondavidson@jabber.org/jabber.org: which are 12 character long with different caps and char
(7:08:58 PM) yohoho@jabber.ccc.de: Linux 2.6.18-274.7.1.el5PAE #1 SMP Thu Oct 20 17:03:59 EDT 2011 i686 i686 i386 GNU/Linux
(7:09:01 PM) yohoho@jabber.ccc.de: if we crack this
(7:09:01 PM) yohoho@jabber.ccc.de: we win
(7:09:07 PM) yohoho@jabber.ccc.de: major target here
(7:09:12 PM) yohoho@jabber.ccc.de: need to root to get 80+ spools tho
(7:12:09 PM) leondavidson@jabber.org/jabber.org: mhm would be nice candidate for local sudo root. vietnamese niggas wrote working exploit that smashes ASLR and other securty shit that comes with redhat these days
(7:14:47 PM) yohoho@jabber.ccc.de: yes that is exactly what is needed
(7:14:49 PM) yohoho@jabber.ccc.de: hold on
(7:15:05 PM) yohoho@jabber.ccc.de: Sudo version 1.7.2p1
(7:15:16 PM) yohoho@jabber.ccc.de: pero necesito valid u/p
(7:15:25 PM) leondavidson@jabber.org/jabber.org: hmm
(7:15:36 PM) yohoho@jabber.ccc.de: # Tod Miller Sudo 1.6.x before 1.6.9p21 and 1.7.x before 1.7.2p4
# local root exploit
# March 2010
# automated by kingcope
(7:15:40 PM) leondavidson@jabber.org/jabber.org: no you dont. the sudo bug is format string in its name
(7:15:54 PM) leondavidson@jabber.org/jabber.org: I'm talking about new sudo root :P
(7:16:09 PM) leondavidson@jabber.org/jabber.org: http://www.vnsecurity.net/2012/02/exploiting-sudo-format-string-vunerability/
(7:16:18 PM) yohoho@jabber.ccc.de: 1.8.0 − 1.8.3 ?
(7:16:22 PM) leondavidson@jabber.org/jabber.org: viet hackers show us how to reproduce it ja
(7:16:38 PM) leondavidson@jabber.org/jabber.org: 1.8.2p1 et al
(7:16:55 PM) yohoho@jabber.ccc.de: hrm
(7:17:00 PM) yohoho@jabber.ccc.de: well this is 1.7.2p1
(7:17:52 PM) leondavidson@jabber.org/jabber.org: ahh
(7:17:54 PM) leondavidson@jabber.org/jabber.org: I see
(7:18:31 PM) leondavidson@jabber.org/jabber.org: hmm hmm hmm
(7:18:58 PM) yohoho@jabber.ccc.de: anyway
(7:19:05 PM) yohoho@jabber.ccc.de: so I was working wth this guy on some shit
(7:19:12 PM) yohoho@jabber.ccc.de: ended up owning a state.gov subdomain
(7:19:20 PM) yohoho@jabber.ccc.de: the SQL DB is like 80+GB
```

(7:19:28 PM) **leondavidson@jabber.org/jabber.org:** holy shit

(7:19:33 PM) **yohoho@jabber.ccc.de:** most of that though is PDFs stored in DB, and ublic PDFs for that matter

(7:19:35 PM) **leondavidson@jabber.org/jabber.org:** the one you were telling me about?

(7:19:39 PM) **leondavidson@jabber.org/jabber.org:** ah lame.

(7:19:44 PM) **yohoho@jabber.ccc.de:** hwoever there are juicy pass lists here

(7:19:53 PM) **leondavidson@jabber.org/jabber.org:** so you already know niggy pass them over

(7:19:56 PM) **leondavidson@jabber.org/jabber.org:** I'll work on crackage

(7:19:57 PM) **yohoho@jabber.ccc.de:** 10,000+ cleartexts + for most major newspapers

(7:20:01 PM) **yohoho@jabber.ccc.de:** cleartexts

(7:20:13 PM) **leondavidson@jabber.org/jabber.org:** SWEET

(7:21:58 PM) **yohoho@jabber.ccc.de:** yeah

(7:22:00 PM) **yohoho@jabber.ccc.de:** this guy canc3r

(7:22:35 PM) **leondavidson@jabber.org/jabber.org:** ja

(7:22:47 PM) **leondavidson@jabber.org/jabber.org:** he hit me up with another sqli for bulgaria.bg or some bulgarian govt shit

(7:22:54 PM) **yohoho@jabber.ccc.de:** I spent many many hours on that shit last night

(7:22:58 PM) **yohoho@jabber.ccc.de:** yeah

(7:23:02 PM) **yohoho@jabber.ccc.de:** he is on jabber now too

(7:23:06 PM) **yohoho@jabber.ccc.de:** canc3r@jabber.org

(7:23:09 PM) **leondavidson@jabber.org/jabber.org:** got you

(7:23:35 PM) **leondavidson@jabber.org/jabber.org:** added him

(7:23:38 PM) **leondavidson@jabber.org/jabber.org:** anyway

(7:23:59 PM) **leondavidson@jabber.org/jabber.org:** what we doing for FFF? just ftc gov box? and the cop shit? that'll be a nice even release

(7:24:09 PM) **yohoho@jabber.ccc.de:** which cop shit ?

(7:24:42 PM) **leondavidson@jabber.org/jabber.org:** nyi/nypdequipment r you gonna hold that for another FFF?

(7:28:00 PM) **yohoho@jabber.ccc.de:** oh fuck yes hold off on that

(7:28:01 PM) **yohoho@jabber.ccc.de:** no where near ready

(7:28:08 PM) **yohoho@jabber.ccc.de:** shit we havent' gotten any mail

(7:28:12 PM) **yohoho@jabber.ccc.de:** havent used their CCs yet

(7:28:18 PM) **leondavidson@jabber.org/jabber.org:** ja

(7:28:47 PM) **leondavidson@jabber.org/jabber.org:** shame we dont have access to main ftc.gov that would been nice

(7:29:15 PM) **yohoho@jabber.ccc.de:** yes

(7:29:17 PM) **yohoho@jabber.ccc.de:** but is different network

(7:31:03 PM) **leondavidson@jabber.org/jabber.org:** ja

(7:58:30 PM) **leondavidson@jabber.org/jabber.org:** jjjjeeeeeeaaaaaaa

(8:01:38 PM) **yohoho@jabber.ccc.de:** any ideas on the other targets?

(8:01:41 PM) **yohoho@jabber.ccc.de:** eagle-us etc ?

(8:04:06 PM) **leondavidson@jabber.org/jabber.org:** what was the latest with that? we got the mails and thats that?

(8:04:18 PM) **yohoho@jabber.ccc.de:** I been doin other shit

(8:04:38 PM) **yohoho@jabber.ccc.de:** we need help to follow through

(8:05:58 PM) **leondavidson@jabber.org/jabber.org:** ill look at it in a few then

(8:06:01 PM) **leondavidson@jabber.org/jabber.org:** see whats goodie

(8:06:20 PM) **leondavidson@jabber.org/jabber.org:** we dont have any other govts to own tomororw? what about all those gov plesks I gave you a wihle back?

(8:06:26 PM) **leondavidson@jabber.org/jabber.org:** well they were kind of small towns and shit nothing exciting

(8:06:38 PM) **yohoho@jabber.ccc.de:** right

(8:06:42 PM) **yohoho@jabber.ccc.de:** some in TX righ ?

(8:06:43 PM) **yohoho@jabber.ccc.de:** there's a few here

(8:06:47 PM) **leondavidson@jabber.org/jabber.org:** ja there were a few

(8:06:52 PM) **leondavidson@jabber.org/jabber.org:** like 10 I gave you a few you rooted

(8:06:54 PM) **leondavidson@jabber.org/jabber.org:** and put to the side

(8:06:55 PM) **leondavidson@jabber.org/jabber.org:** small towns

(8:06:58 PM) **leondavidson@jabber.org/jabber.org:** but .gov's regardless

(8:09:00 PM) **yohoho@jabber.ccc.de:** https://beachcitytx.us:8443/enterprise/control/core.php ls -al /usr/local/psa/qmail/mailnames/

(8:09:04 PM) **yohoho@jabber.ccc.de:** tell me if you find anything interesting in there

(8:11:39 PM) **leondavidson@jabber.org/jabber.org:** got you niglet

(8:39:34 PM) **yohoho@jabber.ccc.de:** hmm?

(9:03:24 PM) **yohoho@jabber.ccc.de:** hmm?

(9:44:52 PM) **yohoho@jabber.ccc.de:** ?

(12:08:46 PM) **leondavidson@jabber.org/4d6c1564f4f96971:** yo what up niglet

(12:08:58 PM) **leondavidson@jabber.org/4d6c1564f4f96971:** do you think this shit is real? http://www.youtube.com/watch?v=umw2JUm0-Lw

(12:09:04 PM) **leondavidson@jabber.org/4d6c1564f4f96971:** or search

(12:09:15 PM) **leondavidson@jabber.org/4d6c1564f4f96971:** "US Soldiers Raping an Iraqi Woman"

(12:09:20 PM) **leondavidson@jabber.org/4d6c1564f4f96971:** uploaded by "truthsyria"

(12:09:25 PM) **leondavidson@jabber.org/4d6c1564f4f96971:** shows u.s solders raping some chick

(12:09:32 PM) **leondavidson@jabber.org/4d6c1564f4f96971:** uploaded/"leaked" today

(12:09:36 PM) **leondavidson@jabber.org/4d6c1564f4f96971:** looks like a bad porno to me

(12:10:33 PM) **leondavidson@jabber.org/4d6c1564f4f96971:** nm looks fake

(12:11:52 PM) **leondavidson@jabber.org/4d6c1564f4f96971:** oh shit you ended up doing the defacements?

(12:11:54 PM) **leondavidson@jabber.org/4d6c1564f4f96971:** wtf no one told me

(12:11:58 PM) **leondavidson@jabber.org/4d6c1564f4f96971:** well I did for asleep

(2:55:17 PM) **leondavidson@jabber.org/jabber.org:** what up foo

(2:55:38 PM) **yohoho@jabber.ccc.de:** back

(2:55:44 PM) **yohoho@jabber.ccc.de:** gotta split in a min tho

(2:55:50 PM) **yohoho@jabber.ccc.de:** yeah we were just like… fuck it

(2:56:01 PM) **yohoho@jabber.ccc.de:** have to follow through on the 'every friday's shit

(2:56:06 PM) **yohoho@jabber.ccc.de:** though other people may also join in on the fun

(2:59:58 PM) **leondavidson@jabber.org/jabber.org:** ja

(3:00:16 PM) **leondavidson@jabber.org/jabber.org:** next time at least write me a message like BOOM GOOD MORNING LOOK AT THIS LOL

(3:00:21 PM) **leondavidson@jabber.org/jabber.org:** I had to find out randomly by reading the news

(3:00:22 PM) **leondavidson@jabber.org/jabber.org:** haha

(3:02:03 PM) **yohoho@jabber.ccc.de:** yo man

(3:02:08 PM) **leondavidson@jabber.org/jabber.org:** yo

(3:02:12 PM) **leondavidson@jabber.org/jabber.org:** dime loco

(3:02:14 PM) **yohoho@jabber.ccc.de:** i'm stressin about this linux target

(3:02:18 PM) **yohoho@jabber.ccc.de:** we _have_ to root this

(3:02:29 PM) **yohoho@jabber.ccc.de:** it has 80+ spools of surveillance corporation

(3:02:29 PM) **leondavidson@jabber.org/jabber.org:** the eagle one?

(3:02:31 PM) **yohoho@jabber.ccc.de:** they do shit for the met

(3:02:42 PM) **yohoho@jabber.ccc.de:** and are doing surveillance for the upcoming G8 / nato

(3:03:06 PM) **leondavidson@jabber.org/jabber.org:** pues vamos a meter mano loco

(3:03:09 PM) **leondavidson@jabber.org/jabber.org:** when you get back hit me up

(3:03:12 PM) **leondavidson@jabber.org/jabber.org:** we'll brainstorm together

(3:03:55 PM) **yohoho@jabber.ccc.de:** ask your 0day homies

(3:03:55 PM) **yohoho@jabber.ccc.de:** Linux 2.6.18-274.7.1.el5PAE #1 SMP Thu Oct 20 17:03:59 EDT 2011 i686 i686 i386 GNU/Linux

(3:04:27 PM) **yohoho@jabber.ccc.de:** now it's running that sudo version Sudo version 1.7.2p1

(3:04:31 PM) **yohoho@jabber.ccc.de:** but I have no valid u/p credential

(3:04:33 PM) **yohoho@jabber.ccc.de:** is cpanel

(3:04:44 PM) **yohoho@jabber.ccc.de:** also they have some firewals, no reverse shells or bindshells

(3:04:53 PM) **yohoho@jabber.ccc.de:** they also have clamav and rkhunter and maybe more IDS type shit

(3:05:10 PM) **yohoho@jabber.ccc.de:** this box is top priority, even more than this state.gov net

(3:05:39 PM) **leondavidson@jabber.org/jabber.org:** mhm

(3:06:10 PM) **yohoho@jabber.ccc.de:** I have a webshell as the permission of the main website's uid, controls all their websites, and a mysql user

(3:06:15 PM) **yohoho@jabber.ccc.de:** nothing really in the DB, just products/categories and like two users, the passwords cracked to 'open'

(3:06:27 PM) **yohoho@jabber.ccc.de:** got in admin panel through injection and upload .php file

(3:08:21 PM) **yohoho@jabber.ccc.de:** this is essential

(3:08:41 PM) **yohoho@jabber.ccc.de:** I believe our best chance at hitting a major surveillance corporation involved in wrongdoing

(3:08:49 PM) **yohoho@jabber.ccc.de:** oh dont know if I told you but I gave JA the third degree

(3:09:00 PM) **leondavidson@jabber.org/jabber.org:** GOOD

(3:09:03 PM) **leondavidson@jabber.org/jabber.org:** he finally came online?

(3:09:22 PM) **yohoho@jabber.ccc.de:** I saw his assistant and I told him to relay the message 'he has a week to deliver or we release shit ourselves'

(3:09:28 PM) **yohoho@jabber.ccc.de:** man that fool came on REAL quick lol

(3:09:42 PM) **yohoho@jabber.ccc.de:** I told him shit was nothing but disappointment

(3:09:44 PM) **yohoho@jabber.ccc.de:** hold on I have log

(3:14:19 PM) **leondavidson@jabber.org/jabber.org:** sweet

(3:14:24 PM) **leondavidson@jabber.org/jabber.org:** hes lucky he aint get on with me

(3:14:30 PM) **leondavidson@jabber.org/jabber.org:** I wanted to blaze that nigga

(3:14:38 PM) **leondavidson@jabber.org/jabber.org:** you know me I'm a beast

(3:15:56 PM) **yohoho@jabber.ccc.de:** dpaeditorial@jabber.ccc.de

please stay calm. everything is going to plan. there are so 50 people working on this now.

ghost

is that so?

we are fully capable of rendering and deploying these emails on our own

dpaeditorial@jabber.ccc.de

go date is within 2 weeks

ghost

you say there is a coalition but we have seen nothing

furthermore you revoke access to what we already had

you realize we are sitting on all this other crazy shit

dpaeditorial@jabber.ccc.de

we work quietly

ghost

results

or we do it ourselves =)

50 people you say? let me in on the ground floor then to see what kind of research they are finding

dpaeditorial@jabber.ccc.de

there are a lot of people all over the world working on this. who will go home if there is any feeling, even for a moment that everything is not going according to plan.

ghost

ok then, where do these people communicate their findings? there is some sort of email list, chatroom? where is the email search portal that they are using?

strategy sessions? we'd like in.

dpaeditorial@jabber.ccc.de

please do not contact random people and mention anything about what is happening

ghost

oh please have we not been entirely cooperative with the bizarre restrictions you have set in place?

you said a month when we initially handed it over

we've been moved on to other bigass targets

dpaeditorial@jabber.ccc.de

if for some reason i am uncontactable you can ask around for me, but never mention the target, go dates, etc

ghost

yawn

one week

or we release ourselves

dpaeditorial@jabber.ccc.de

we've had a few distractions ;)

we have a complex political timetable we have assessed. other events in a week will distract and minimize the impact.

ghost

like what?

why are you not including any of us in on these strategy sessions ?

dpaeditorial@jabber.ccc.de
the G8
ghost
yes and having connections with folks on the ground in texas who are very curious about stratfor, and having connections with organizers in chicago, there are people wanting to see what is in this hsit
dpaeditorial@jabber.ccc.de
we know how to maximize impact. we've spent a lot of time on this.
ghost
ok so what have you found so far ?
dpaeditorial@jabber.ccc.de
dont fuck it.
there's too much to describe. i am not searching for anything. i am managing 20 organizations each with their own journalists.
areas where i know the detail, are too explosive to reveal.
ghost
ok then, you are communicating with all those people, but not with us, and not us directly with them either for that matter
we need to see some public release of some fo your findings within a week
dpaeditorial@jabber.ccc.de
i dont even communicate with the other orgs
our people do that.
i communicate with them
but I dont like to pass sources onto anyone else. i trust only myself.
there will be no release within a week. whoś idea is that?
ghost
there is concern that this is elaborate hoax on yall part
we don't like to sit on unreleased data this long
dpaeditorial@jabber.ccc.de
we have a complex battle plan. dont fuck
ghost
yeah I'm not convinced.
one week or else we render ourselves
release something to the public in a week
furthermore, give us access to your current search engine
I have friends who have already been alluded to being mentioned in these emails who want to verify
dpaeditorial@jabber.ccc.de
we wont do that. we have a press conference booked. there are front pages being ready. it is not possible to change the course of such a big ship.
ghost
ok then how long
dpaeditorial@jabber.ccc.de
under 2 weeks
ghost
ok

then hook us up with your current search engine
if you can guarantee 2 weeks and provide the search engine, we will be patient and see what happens until then
dpaeditorial@jabber.ccc.de
we removed access to the previous one because the big ship was splitting appart because things were pasted on pastebin and people were saying "fuck thing" because, for example they were working on a big splash on occupy
so their efforts were ruined, because their editors said it wasnt new anymore
ghost
their efforts wouldnt have existed if we didnt steal the emails ourselves
dpaeditorial@jabber.ccc.de
I'll speak later tonight
ghost
yall need to keep up with us
dpaeditorial@jabber.ccc.de
of course.
ghost
we have so much more on the way
and when considering how we will release, you're not on top of list
dpaeditorial@jabber.ccc.de
I know that.
ghost
I will push it back to 2 weeks and we will stay quiet, but you need to guarantee results
dpaeditorial@jabber.ccc.de
But we know how to do this. If you have someone who has a deep attention span and can keep their mouth shut and themselves, and others secure, then they can help research for the anon stories.
ghost
no one more qualified than me
dpaeditorial@jabber.ccc.de
you have some leverage here. but dont abuse it.
we want the same thing. dont fuck it up and we all get the biggest possible bang.
ghost
great, then make it happen
and yes, i'd like to help research the materials, specifically about anon, anarchists, occupy, greece, and G8
grep takes forever, and I'd render the shit myself, but I am in the middle of owning big governments and digital surveillance corporations
dpaeditorial@jabber.ccc.de
yup. comaritive advantage. we all do what we do best and help each other.
ghost
k
dpaeditorial@jabber.ccc.de
the most organized, coherent group will win
i have to relocate now. will try to be around more
bye!

(3:18:04 PM) **yohoho@jabber.ccc.de:** but yo
(3:18:08 PM) **yohoho@jabber.ccc.de:** i'm serious about trying to root this shit
(3:18:13 PM) **yohoho@jabber.ccc.de:** if we have to trade or wahtever to get what we need out of this
(3:18:27 PM) **yohoho@jabber.ccc.de:** i'm having nightmares about missing the opportunity on this box
(3:18:35 PM) **leondavidson@jabber.org/jabber.org:** we wont nigga. I won't let you down
(3:18:40 PM) **leondavidson@jabber.org/jabber.org:** I'm on the move today
(3:18:49 PM) **leondavidson@jabber.org/jabber.org:** reaching out to all my sec researchers
(3:19:00 PM) **yohoho@jabber.ccc.de:** here are all the suid binaries on the box
(3:19:01 PM) **yohoho@jabber.ccc.de:** /usr/local/apache.backup/bin/suexec

```
/usr/local/apache.backup_archive/20090114.1231891935/bin/suexec
/usr/local/apache/bin/suexec
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/at
/usr/bin/screen
/usr/bin/sudoedit
/usr/bin/wall
/usr/bin/chfn
/usr/bin/ssh-agent
/usr/bin/crontab
/usr/bin/write
/usr/bin/chage
/usr/bin/quota
/usr/sbin/sendmail
/usr/sbin/exim
/usr/sbin/usernetctl
/usr/sbin/userhelper
/usr/libexec/openssh/ssh-keysign
/usr/libexec/dell_dup/dell_ie_zappa-1.0.8/xmloutput.xml
/usr/libexec/dell_dup/dell_ie_zappa-1.0.8/PV2XX.log
/usr/libexec/utempter/utempter
/bin/mount
/bin/umount
/bin/ping
/bin/su
/bin/ping6
/sbin/unix_chkpwd
/sbin/pam_timestamp_check
/sbin/umount.nfs
/sbin/umount.nfs4
/sbin/netreport
/sbin/mount.nfs4
```

/sbin/mount.nfs
/opt/dell/srvadmin/sbin/omcliproxy
/opt/suphp/sbin/suphp
/opt/arkeia/arkeiad/arkfs/arkfs_exclude.lst
/var/cpanel/rvglobalsoft/rvsitebuilder/rvbin/rvswrapper
/lib/dbus-1/dbus-daemon-launch-helper

(3:19:34 PM) **leondavidson@jabber.org/jabber.org:** hows versions looking on glibc/libc. what else is running root on the box?

(3:20:00 PM) **yohoho@jabber.ccc.de:** I tried the LD_AUDIT trickk

(3:20:02 PM) **leondavidson@jabber.org/jabber.org:** ja

(3:20:08 PM) **yohoho@jabber.ccc.de:** but maybe I will have to try oit in a more interactive setting

(3:20:28 PM) **leondavidson@jabber.org/jabber.org:** lets also look at those other weird suids. rvswrapper and so on

(3:20:38 PM) **yohoho@jabber.ccc.de:** im not gonna get n the box right now

(3:20:42 PM) **leondavidson@jabber.org/jabber.org:** /usr/libexec/dell_dup/dell_ie_zappa-1.0.8/xmloutput.xml
/usr/libexec/dell_dup/dell_ie_zappa-1.0.8/PV2XX.log these files are suid why?

(3:20:46 PM) **yohoho@jabber.ccc.de:** I really believe they are tightly monitoring this box

(3:20:56 PM) **leondavidson@jabber.org/jabber.org:** kk

(3:21:52 PM) **yohoho@jabber.ccc.de:** yeah no idea

(3:22:00 PM) **yohoho@jabber.ccc.de:** there appears to be some dell server admin shit on this

(3:22:26 PM) **yohoho@jabber.ccc.de:** hhold on look at this ps -aux

(3:22:29 PM) **leondavidson@jabber.org/jabber.org:** kk

(3:22:51 PM) **yohoho@jabber.ccc.de:** and you will see what I mean

(3:24:53 PM) **yohoho@jabber.ccc.de:** did you get that

(3:24:57 PM) **yohoho@jabber.ccc.de:** or did it kill my otr

(3:25:20 PM) **leondavidson@jabber.org/jabber.org:** killed otr

(3:25:29 PM) **yohoho@jabber.ccc.de:** ok I will cryptobin

(3:26:01 PM) **leondavidson@jabber.org/jabber.org:** kk

(3:26:18 PM) **yohoho@jabber.ccc.de:** https://cryptobin.org/m4k7g3o0 pass jaja

(3:26:23 PM) **yohoho@jabber.ccc.de:** dont give this out because it contains name of target

(3:27:32 PM) **leondavidson@jabber.org/jabber.org:** I don't give shit out homey you know this.

(3:33:01 PM) **leondavidson@jabber.org/jabber.org:** yumm

(3:33:06 PM) **leondavidson@jabber.org/jabber.org:** I love these kind of boxes

(3:33:14 PM) **leondavidson@jabber.org/jabber.org:** hows your perms on /data01/ filesystem?

(3:33:22 PM) **leondavidson@jabber.org/jabber.org:** is it some nas type shit? or NFS mount to another server?

(3:33:23 PM) **yohoho@jabber.ccc.de:** can't even list data01/

(3:33:25 PM) **yohoho@jabber.ccc.de:** that is user home dir

(3:33:28 PM) **leondavidson@jabber.org/jabber.org:** mm

(3:33:31 PM) **yohoho@jabber.ccc.de:** nope

(3:33:33 PM) **yohoho@jabber.ccc.de:** I think it is local

(3:33:36 PM) **yohoho@jabber.ccc.de:** mounted separately tho

(3:33:38 PM) **yohoho@jabber.ccc.de:** or something

(3:33:39 PM) **yohoho@jabber.ccc.de:** but

(3:33:44 PM) **yohoho@jabber.ccc.de:** can only read home dir there

(3:33:54 PM) **yohoho@jabber.ccc.de:** I can list /mail01/ etc lotsa spools but can't go in
(3:34:01 PM) **yohoho@jabber.ccc.de:** cpanel locoks shit down to each user pretty well
(3:34:08 PM) **leondavidson@jabber.org/jabber.org:** hows your perms on /usr/local/zen/monitor directory structure? these are perl scripts running as root
(3:34:20 PM) **leondavidson@jabber.org/jabber.org:** check to see if they use suidperl and you can inherit root, or if any of them are writable
(3:35:59 PM) **leondavidson@jabber.org/jabber.org:** /usr/sbin/pure-uploadscript -B -r /etc/cxs/cxsftp.sh <-- look at this shell script. verify what it is doing and if we got perms for it
(3:36:34 PM) **yohoho@jabber.ccc.de:** can't go into cxs
(3:36:41 PM) **yohoho@jabber.ccc.de:** can't view that script or anything in taht dir
(3:36:47 PM) **yohoho@jabber.ccc.de:** I can view the monitor scripts
(3:36:49 PM) **leondavidson@jabber.org/jabber.org:** /opt/arkeia/bin/arkpsys -S 3 -h localhost -u root -s ARKPSYS -R = I want to look into this. interesting script running as root under user root
(3:36:54 PM) **yohoho@jabber.ccc.de:** they are called through cron I believe
(3:37:02 PM) **leondavidson@jabber.org/jabber.org:** lets see what some of these are doing im sure you checked cron yes?
(3:37:07 PM) **yohoho@jabber.ccc.de:** yes h had some ideas about that
(3:37:13 PM) **yohoho@jabber.ccc.de:** yes I did they run mostly av and monitoring shit
(3:37:21 PM) **yohoho@jabber.ccc.de:** nothing that I could execute though
(3:37:27 PM) **yohoho@jabber.ccc.de:** err change I mean
(3:37:48 PM) **leondavidson@jabber.org/jabber.org:** mm
(3:43:12 PM) **leondavidson@jabber.org/jabber.org:** http://wiki.arkeia.com/mediawiki/index.php/Security_Guide reading about script
(4:16:58 PM) **leondavidson@jabber.org/jabber.org:** look into that /opt/arkeia directory for arkc.param
(4:17:06 PM) **leondavidson@jabber.org/jabber.org:** find /opt/arkeia -name arkc.param
(4:17:14 PM) **leondavidson@jabber.org/jabber.org:** if its readable should contain some config like passwords
(4:19:15 PM) **yohoho@jabber.ccc.de:** I will check later
(4:19:23 PM) **yohoho@jabber.ccc.de:** did you look at those TX servers ?
(4:19:24 PM) **yohoho@jabber.ccc.de:** I have to split
(4:19:29 PM) **yohoho@jabber.ccc.de:** we need your help
(4:19:34 PM) **yohoho@jabber.ccc.de:** need to get your hands dirty homey
(4:19:39 PM) **leondavidson@jabber.org/jabber.org:** ja
(4:19:41 PM) **yohoho@jabber.ccc.de:** I can't carry this all myself
(4:19:48 PM) **leondavidson@jabber.org/jabber.org:** lets work on it tonight
(4:19:55 PM) **leondavidson@jabber.org/jabber.org:** see your ass later niggy
(4:19:58 PM) **yohoho@jabber.ccc.de:** k
(7:21:32 PM) **yohoho@jabber.ccc.de:** -rw------- 1 root root 2212 Jun 7 2011 /opt/arkeia/arkc/arkc.param