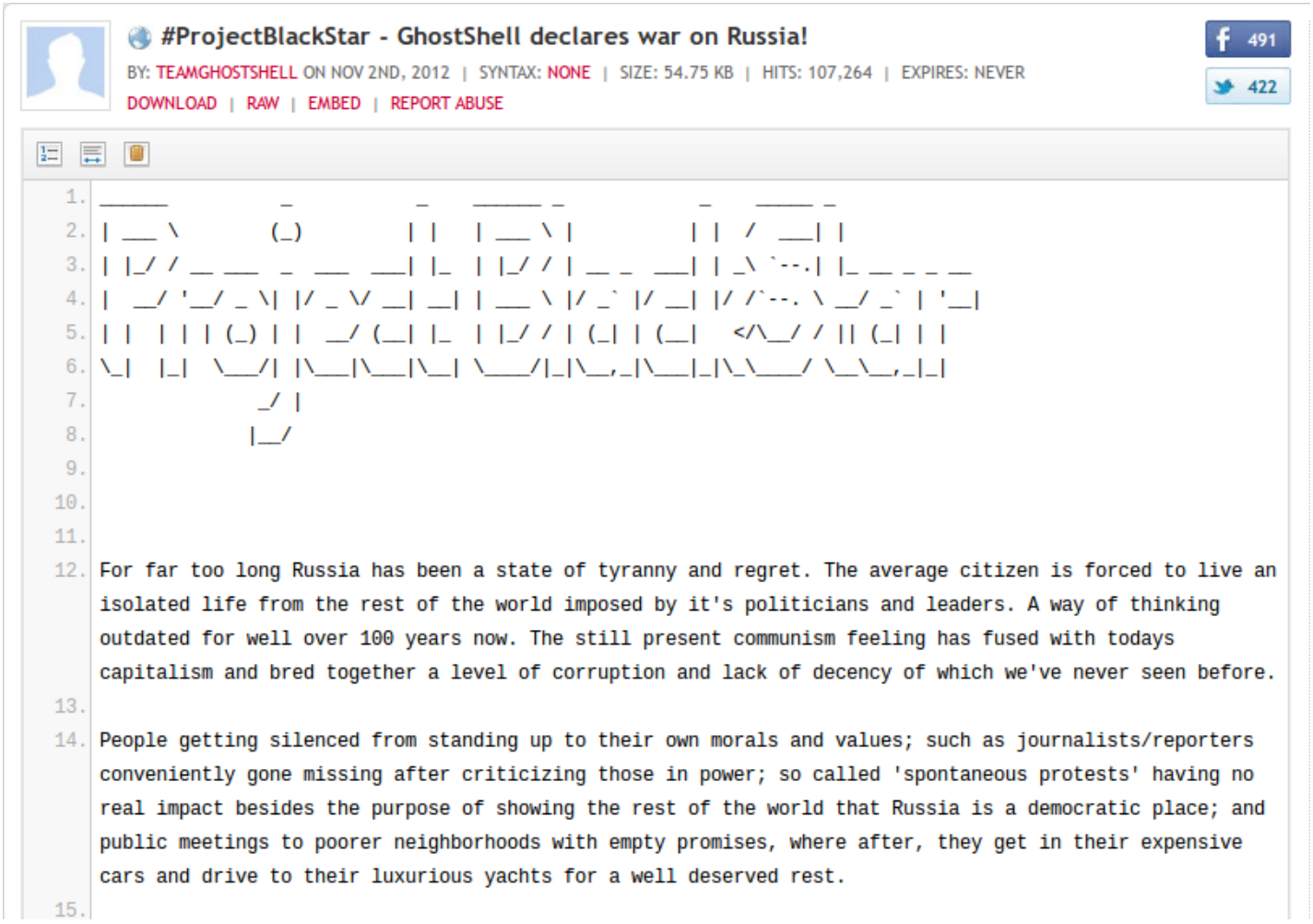
Whats to see in BlackStar?

On November 2nd 2012, the Ghostshell hacker group released a rather large dump of records from various Russian companies. The original link is http://pastebin.com/yXN7uc6r, but in case it disappears, here is the gist of it:



So being the inquisitive sort, I figured let me take a look at this dump and see what I could see. First off I had to get the data, a combination of *wget* and *links* helped with that. Then I started looking around. Now please bear in mind, this is what I found. In all probablity I missed some items just due to the sheer amount of data to work through. With that out of the way..

Email addresses
I wondered about the email addresses in use according to these dumps. I found a total of 234498 email addresses, there are of course a lot of *.ru* domains (duh) and the normal contenders:

```
Top 20 email domains:
    374 pochta.ru
    376 yandex.com
    385 ukr.net
    593 gawab.com
    636 mawpinkow.konin.pl
    654 o2.pl
    892 yahoo.co.uk
    893 yahoo.com
    900 hotmail.com
   1021 ourstorereviews.org
```

```
  1550 ya.ru
  3717 inbox.ru
  4502 list.ru
  5426 aol.com
  5692 bk.ru
  5917 gold-standard.ru
 11233 rambler.ru
 28006 yandex.ru
 39156 gmail.com
 73466 mail.ru
```

Then I thought, what about the always interesting *.edu / .gov / .mil* addresses?

```
     1 astillero.gba.gov
     1 az4871.spb.edu
     1 cc.tpu.edu
     1 crimea.edu
     1 dhe.tpu.edu
     1 fnsm.tpu.edu
     1 gatech.edu
     1 indiana.edu
     1 nowy.lorenz.edu
     1 nw.ksaa.edu
     1 ruvkmooeki.edu
     1 supersada.edu
     1 us.army.mil
     1 yrbkmooehf.edu
     2 seo.lorenz.edu
     2 sjsu.edu
     6 istu.edu
    10 phystech.edu
```

What about funny stuff? Things like:

```
     1 ringl68b02-platinum-gmail.com
     1 ringwlanhccvmmuxc-platinum-gmail.com
     1 ringwljy2399-platinum-gmail.com
     1 ringwxmhwadhvih-platinum-gmail.com
     7 googlemails.net

     1 mazila-firefox.org.ua
     1 mozilla-firefox-ru.ru

     1 freeemailyahoo.com
     1 yyahoo.es

     1 adobe-acrobat-reader.ru
     1 adobe-reader-acrobat.ru

     1 findpharmasolutions2010.co.cc
     1 makizpharma.ru
     1 mdpharmacy.net
     1 pharmaceuticalprocesssystems.co.cc
     1 pharmacy-city.com
     1 pharmacy-ed.info
     1 pharmagarant.ru
     1 pharmateca.ru
```

```
      1 polpharma.ru
      1 resopharma.fr
      1 xenopharmacophilia.com
      2 canonpharma.ru
      3 conventpharma.ru
      3 friendpharmacy.com
      4 pharmalin.com
```

As a case in point, lets look at *yyahoo.es*:

```
Yyahoo.es Server Details
IP address: 46.105.140.156
Server Location: France
ISP: Ovh Systems

IP address :    46.105.140.156
IP country code:    FR
IP address country:     France
IP address state:     n/a
IP address city:     n/a
IP address latitude:     46.0000
IP address longitude:     2.0000
ISP of this IP :     Ovh Systems
Organization:     Servidores vps
Host of this IP:      parking1.cathedralsoft.com
```

..so not looking as if yahoo has anything to do with that domain. Here is the sorted and counted list of email domains (here) if you want to take a look.

Unencrypted passwords
The next step was to see if there were any passwords in the dumps. But here i mean plaintext passwords, you know, when the company or site did not even do hashing but just wrote it straight to a database field. Well I found 52393 unique passwords, needless to say there were many repeats before I did the sort. The list is here, but I also ran a dictionary analyzer (*pipal*) against it:

```
Top 10 base words
qwerty = 35 (0.07%)
password = 25 (0.05%)
alex = 21 (0.04%)
melto = 17 (0.03%)
skills = 13 (0.02%)
pass = 13 (0.02%)
mama = 12 (0.02%)
olga = 12 (0.02%)
qwert = 11 (0.02%)
qwer = 10 (0.02%)

Password length (length ordered)
1 = 9 (0.02%)
2 = 19 (0.04%)
3 = 137 (0.26%)
4 = 573 (1.09%)
5 = 627 (1.2%)
6 = 3217 (6.14%)
7 = 2874 (5.49%)
8 = 4245 (8.1%)
9 = 4833 (9.22%)
```

10 = 32520 (62.07%)
11 = 1174 (2.24%)
12 = 839 (1.6%)
13 = 499 (0.95%)
14 = 295 (0.56%)
15 = 162 (0.31%)
16 = 150 (0.29%)
17 = 54 (0.1%)
18 = 54 (0.1%)
19 = 15 (0.03%)
20 = 40 (0.08%)
21 = 6 (0.01%)
22 = 14 (0.03%)
23 = 2 (0.0%)
24 = 5 (0.01%)
26 = 4 (0.01%)
27 = 2 (0.0%)
28 = 2 (0.0%)
30 = 1 (0.0%)
32 = 3 (0.01%)
33 = 1 (0.0%)
34 = 5 (0.01%)
35 = 1 (0.0%)
36 = 1 (0.0%)
37 = 2 (0.0%)
38 = 2 (0.0%)
40 = 2 (0.0%)
53 = 1 (0.0%)
57 = 1 (0.0%)
58 = 1 (0.0%)
67 = 1 (0.0%)

Password length (count ordered)
10 = 32520 (62.07%)
9 = 4833 (9.22%)
8 = 4245 (8.1%)
6 = 3217 (6.14%)
7 = 2874 (5.49%)
11 = 1174 (2.24%)
12 = 839 (1.6%)
5 = 627 (1.2%)
4 = 573 (1.09%)
13 = 499 (0.95%)
14 = 295 (0.56%)
15 = 162 (0.31%)
16 = 150 (0.29%)
3 = 137 (0.26%)
17 = 54 (0.1%)
18 = 54 (0.1%)
20 = 40 (0.08%)
2 = 19 (0.04%)
19 = 15 (0.03%)
22 = 14 (0.03%)
1 = 9 (0.02%)
21 = 6 (0.01%)
34 = 5 (0.01%)

```
24 = 5 (0.01%)
26 = 4 (0.01%)
32 = 3 (0.01%)
27 = 2 (0.0%)
38 = 2 (0.0%)
28 = 2 (0.0%)
37 = 2 (0.0%)
23 = 2 (0.0%)
40 = 2 (0.0%)
30 = 1 (0.0%)
33 = 1 (0.0%)
53 = 1 (0.0%)
35 = 1 (0.0%)
36 = 1 (0.0%)
58 = 1 (0.0%)
67 = 1 (0.0%)
57 = 1 (0.0%)

          |
          |
          |
          |
          |
          |
          |
          |
          |
          |
          |
          |
          |
        |||
      |||||
|||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||
0000000000111111111122222222223333333333444444444455555555556666666666
0123456789012345678901234567890123456789012345678901234567890123456789012345678

One to six characters = 4582 (8.75%)
One to eight characters = 11701 (22.33%)
More than eight characters = 40692 (77.67%)

Only lowercase alpha = 5949 (11.35%)
Only uppercase alpha = 324 (0.62%)
Only alpha = 6273 (11.97%)
Only numeric = 2055 (3.92%)

First capital last symbol = 16 (0.03%)
First capital last number = 8376 (15.99%)

Months
march = 4 (0.01%)
april = 2 (0.0%)
may = 16 (0.03%)
july = 3 (0.01%)
august = 1 (0.0%)
september = 1 (0.0%)
```

october = 1 (0.0%)

Days
None found

Months (Abreviated)
jan = 23 (0.04%)
feb = 5 (0.01%)
mar = 142 (0.27%)
apr = 31 (0.06%)
may = 16 (0.03%)
jun = 19 (0.04%)
jul = 28 (0.05%)
aug = 7 (0.01%)
sept = 2 (0.0%)
oct = 9 (0.02%)
nov = 55 (0.1%)
dec = 10 (0.02%)

Days (Abreviated)
mon = 48 (0.09%)
wed = 9 (0.02%)
fri = 15 (0.03%)
sat = 22 (0.04%)
sun = 19 (0.04%)

Includes years
1975 = 11 (0.02%)
1976 = 19 (0.04%)
1977 = 24 (0.05%)
1978 = 20 (0.04%)
1979 = 28 (0.05%)
1980 = 36 (0.07%)
1981 = 21 (0.04%)
1982 = 27 (0.05%)
1983 = 23 (0.04%)
1984 = 42 (0.08%)
1985 = 25 (0.05%)
1986 = 25 (0.05%)
1987 = 34 (0.06%)
1988 = 24 (0.05%)
1989 = 18 (0.03%)
1990 = 11 (0.02%)
1991 = 18 (0.03%)
1992 = 8 (0.02%)
1993 = 4 (0.01%)
1994 = 11 (0.02%)
1995 = 3 (0.01%)
1996 = 2 (0.0%)
1997 = 8 (0.02%)
1998 = 4 (0.01%)
1999 = 2 (0.0%)
2000 = 14 (0.03%)
2001 = 16 (0.03%)
2002 = 7 (0.01%)
2003 = 7 (0.01%)

2004 = 13 (0.02%)
2005 = 24 (0.05%)
2006 = 20 (0.04%)
2007 = 23 (0.04%)
2008 = 20 (0.04%)
2009 = 29 (0.06%)
2010 = 52 (0.1%)
2011 = 61 (0.12%)
2012 = 29 (0.06%)
2013 = 2 (0.0%)
2014 = 2 (0.0%)
2015 = 4 (0.01%)
2017 = 2 (0.0%)
2018 = 2 (0.0%)
2019 = 2 (0.0%)
2020 = 5 (0.01%)

Years (Top 10)
2011 = 61 (0.12%)
2010 = 52 (0.1%)
1984 = 42 (0.08%)
1980 = 36 (0.07%)
1987 = 34 (0.06%)
2012 = 29 (0.06%)
2009 = 29 (0.06%)
1979 = 28 (0.05%)
1982 = 27 (0.05%)
1985 = 25 (0.05%)

Colours
black = 10 (0.02%)
blue = 3 (0.01%)
green = 11 (0.02%)
orange = 1 (0.0%)
pink = 3 (0.01%)
red = 46 (0.09%)
white = 4 (0.01%)
violet = 1 (0.0%)
indigo = 1 (0.0%)

Single digit on the end = 1493 (2.85%)
Two digits on the end = 1607 (3.07%)
Three digits on the end = 16176 (30.87%)

Last number
0 = 619 (1.18%)
1 = 3021 (5.77%)
2 = 2774 (5.29%)
3 = 2932 (5.6%)
4 = 2791 (5.33%)
5 = 2819 (5.38%)
6 = 2651 (5.06%)
7 = 2738 (5.23%)
8 = 2825 (5.39%)
9 = 2691 (5.14%)

Last digit
1 = 3021 (5.77%)
3 = 2932 (5.6%)
8 = 2825 (5.39%)
5 = 2819 (5.38%)
4 = 2791 (5.33%)
2 = 2774 (5.29%)
7 = 2738 (5.23%)
9 = 2691 (5.14%)
6 = 2651 (5.06%)
0 = 619 (1.18%)

Last 2 digits (Top 10)
88 = 573 (1.09%)
23 = 545 (1.04%)
11 = 489 (0.93%)
12 = 436 (0.83%)
77 = 402 (0.77%)
45 = 370 (0.71%)
56 = 356 (0.68%)
89 = 353 (0.67%)
21 = 334 (0.64%)
55 = 328 (0.63%)

Last 3 digits (Top 10)
123 = 296 (0.56%)
111 = 114 (0.22%)
777 = 103 (0.2%)
234 = 96 (0.18%)
345 = 86 (0.16%)
321 = 86 (0.16%)
456 = 83 (0.16%)
789 = 71 (0.14%)
984 = 62 (0.12%)
011 = 59 (0.11%)

Last 4 digits (Top 10)
1234 = 64 (0.12%)

2011 = 47 (0.09%)
2345 = 46 (0.09%)
3456 = 45 (0.09%)
2010 = 43 (0.08%)
1984 = 36 (0.07%)
1980 = 30 (0.06%)
1987 = 27 (0.05%)
2009 = 26 (0.05%)
1979 = 24 (0.05%)

Last 5 digits (Top 10)
23456 = 41 (0.08%)
12345 = 35 (0.07%)
54321 = 12 (0.02%)
56789 = 12 (0.02%)
23123 = 10 (0.02%)
34567 = 10 (0.02%)
11111 = 9 (0.02%)
45678 = 7 (0.01%)
77777 = 7 (0.01%)
55555 = 6 (0.01%)

US Area Codes
234 = NE Ohio: Canton, Akron (OH)
345 = Cayman Islands (--)
321 = Florida: Brevard County, Cape Canaveral area; Metro Orlando (FL)
456 = Inbound International (--)
984 = E North Carolina: Raleigh (NC)

Character sets
mixedalphanum: 33894 (64.69%)
loweralphanum: 7361 (14.05%)
loweralpha: 5949 (11.35%)
numeric: 2055 (3.92%)
mixedalpha: 1455 (2.78%)
upperalphanum: 535 (1.02%)
upperalpha: 324 (0.62%)
loweralphaspecial: 129 (0.25%)
loweralphaspecialnum: 91 (0.17%)
mixedalphaspecialnum: 66 (0.13%)
specialnum: 46 (0.09%)
upperalphaspecial: 20 (0.04%)
mixedalphaspecial: 17 (0.03%)
upperalphaspecialnum: 11 (0.02%)
special: 1 (0.0%)

Character set ordering
othermask: 25614 (48.89%)
stringdigit: 10588 (20.21%)
allstring: 7728 (14.75%)
stringdigitstring: 3357 (6.41%)
alldigit: 2055 (3.92%)
digitstringdigit: 1910 (3.65%)
digitstring: 944 (1.8%)
stringspecialstring: 118 (0.23%)
stringspecialdigit: 44 (0.08%)

```
stringspecial: 24 (0.05%)
specialstring: 8 (0.02%)
specialstringspecial: 2 (0.0%)
allspecial: 1 (0.0%)

Hashcat masks (Top 10)
?l?l?l?l?l?l: 1252 (2.39%)
?l?l?l?l?l?l?l?l?l: 1058 (2.02%)
?l?l?l?l?l?l?l?l: 1037 (1.98%)
?l?l?l?l?l?l?l: 972 (1.86%)
?d?d?d?d?d?d: 788 (1.5%)
?d?d?d?d?d?d?d?d: 500 (0.95%)
?l?l?l?l?l: 401 (0.77%)
?l?l?l?l?l?l?l?l?l: 354 (0.68%)
?l?l?l?l: 266 (0.51%)
?d?d?d?d?d?d?d: 225 (0.43%)
```

Encrypted passwords
Lastly, I looked for passwords hashes. I found three types *MD5 / SHA1 / MYSQL*, more specifically:

MD5	3555	blackstar-encode-1.hash (get it here)
SHA1	2389	blackstar-encode-2.hash (get it here)
MYSQL	4262	blackstar-encode-3.hash (get it here)
10206 total		

I had a quick run through the hashes to see what I could quickly crack:

MD5	1261 left of 3555
SHA1	1131 left of 2389
MYSQL	486 left of 4262
7328 out 10206 done, 71% done	

I will do the dictionary analysis when I get to more then 80% on them. But if you want the dictionary file of progress so far, get it here.

More coming as I get through more of the hashes.

Update - 12-Dec-2012:
I have moved all new progress to a page specifically for hashdumps and cracking them. Please go there for the latest progress and dictionary.