



# **Yandex reward program**

## **ONsec experience**

DEFCON Russia, DCG-7812

21/02/2013 Saint-Petersburg, Yandex

# History of Yandex rewards

- 2011, October - November: Yandex's Month of Security Bugs
- Prizes:
  - 1-st @d0znpp (@ONsec\_Lab)
  - 2-nd @ASintsov
  - 3-rd @kyprizel (now in Yandex team)

# History of Yandex rewards

- 2011, October - November: Yandex's Month of Security Bugs
- Bugs:
  - 1-st Massive XXE
  - 2-nd Auth bypass at mail service
  - 3-rd CSRF/XSS collection at auth system

# What about now?

- Bug bounty program every time
- <http://company.yandex.com/security/>
- From \$100 (A06,10) to \$1000 (A01) per bug
- OWASP Top-10 based rating

# @ONsec\_Lab bugs stats

Only server-side - only hardcode!!!

- 20 bugs accepted
- 1 reject as a double
- 11 qualified bugs
- 9 bugs at progress
- 240'000 rub approved, 80'000 paid rewards
- 21'818 rub per bug average (\$715)

# What about bugs?

All our bugs are server-side:

- XXE against - nothing interesting
- Memcached injections through SSRF
- Nice "RCE" story
- Great SSRFs for HITB2013AMS (not now)

# Memcached injection through SSRF

- All theory described at our ZeroNights

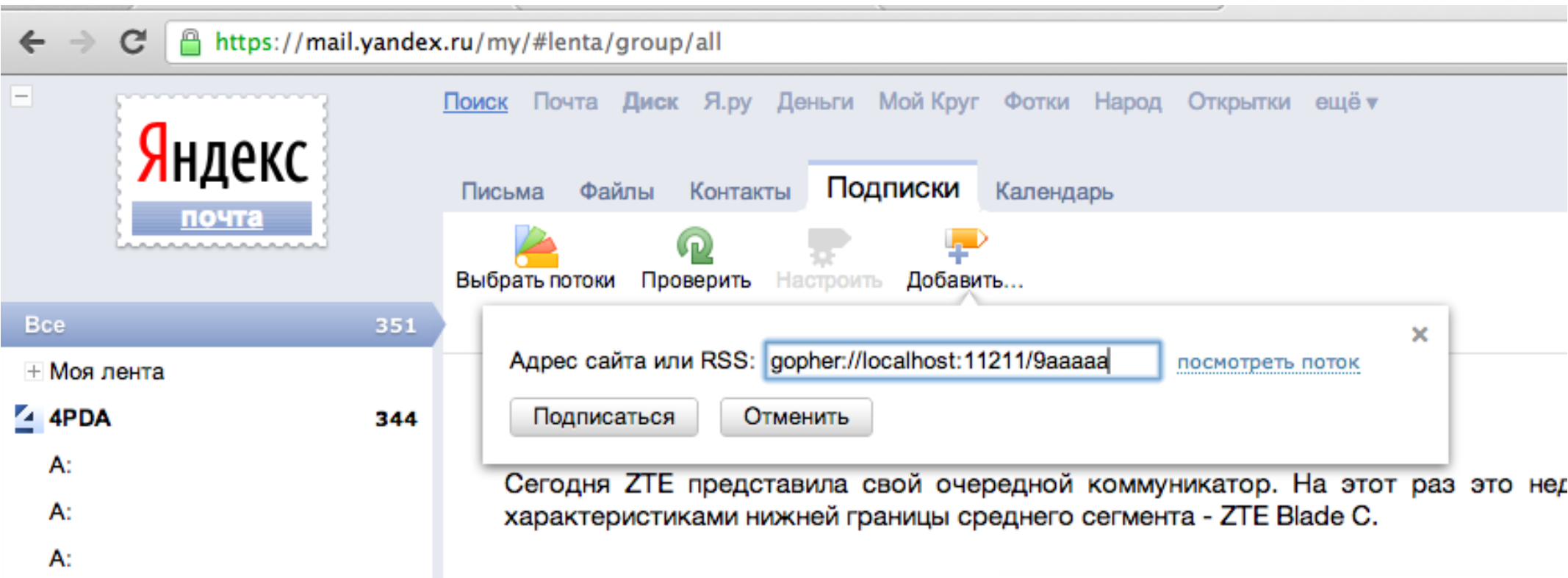
report: [www.slideshare.net/d0znpp/ssrf-attacks-and-sockets-smorgasbord-of-vulnerabilities](http://www.slideshare.net/d0znpp/ssrf-attacks-and-sockets-smorgasbord-of-vulnerabilities)

- Find possibility to write in sockets:

ANYPREFIX\nyoudata\nANYPOSTFIX

- Write it to localhost 11211 port - easy!

# Memcached injection through SSRF





# Nice "RCE" story: stages

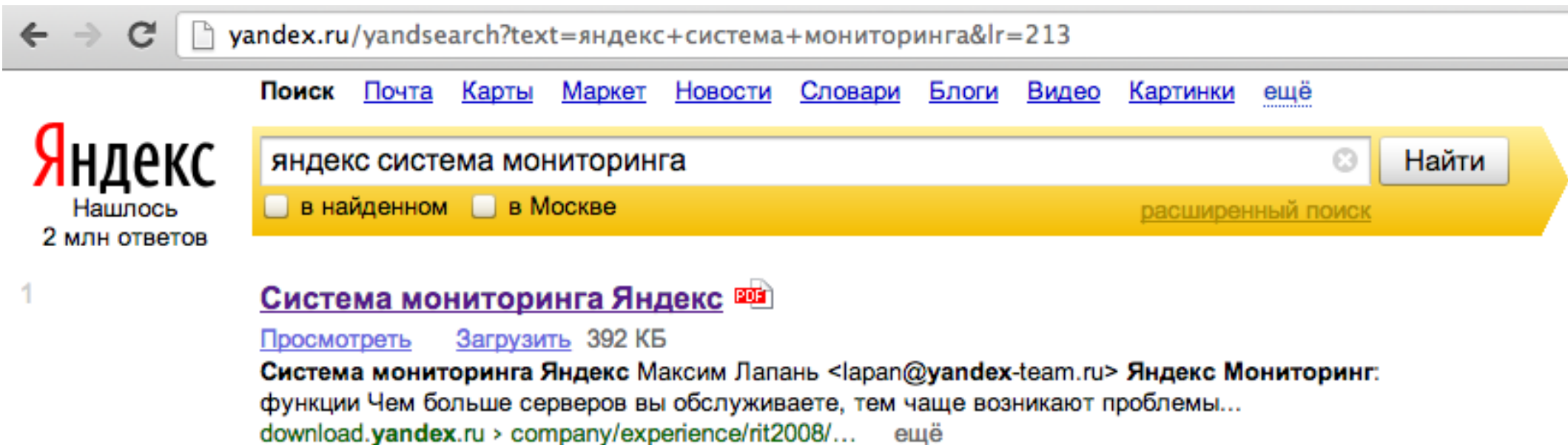
- Determine target
- Find information leaks
- Find vulns
- Find SSRF to exploit vulns
- Exploit vuln through SSRF

# Determine target

- Have connections from anywhere in infrastructure
- Have information about all infrastructure
- Monitoring system!

# Find information leaks

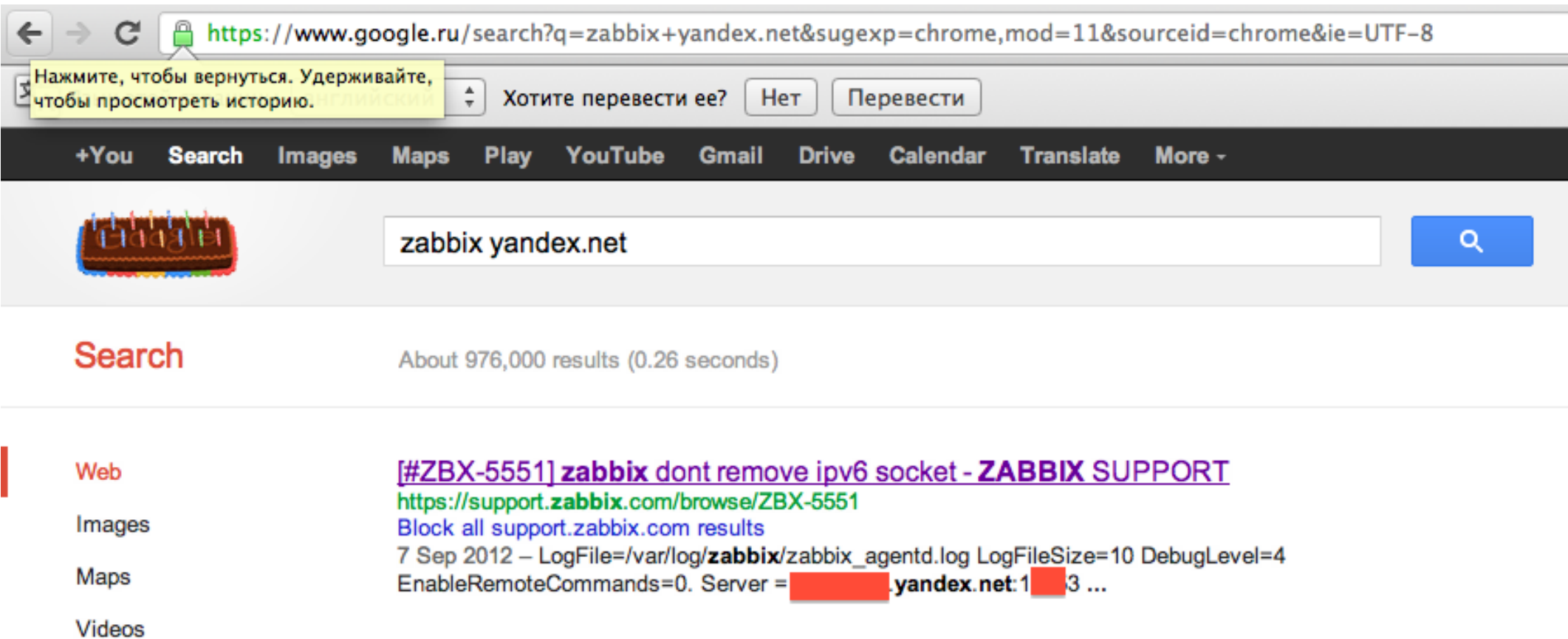
- Use Yandex to hack Yandex:



- This presentation contain info about Zabbix

# Find information leaks

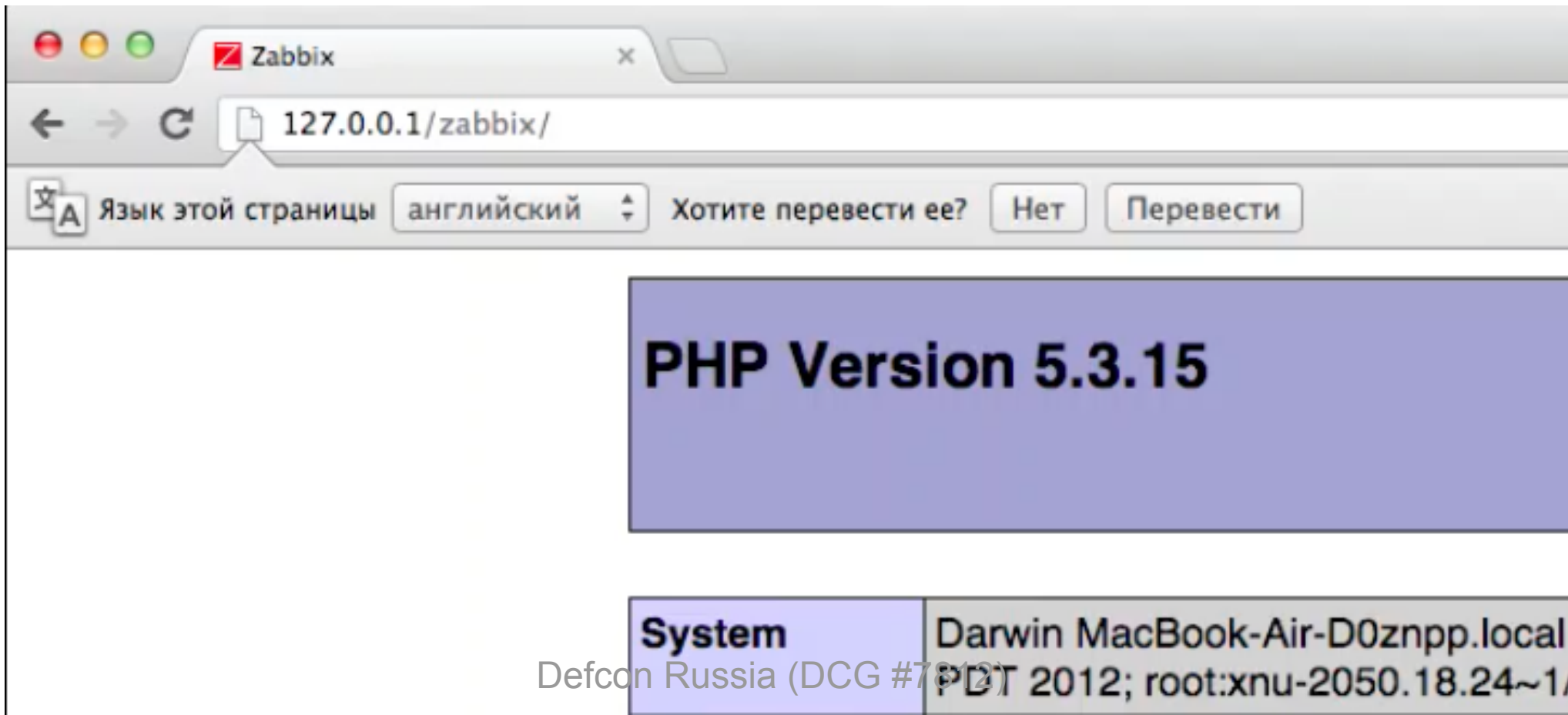
- Use Google to hack Yandex:



- This ticket contained intranet host of Zabbix in Yandex

# Find vulns in Zabbix

- Zabbix RCE vulnerability were found
- Presented at **ZeroNights 0day show**



## HAProxy version 1.15, released 2011/04/08

Statistics Report for pid 26731

- ```
pid = 26731 (process #1, nbproc = 1)
uptime = 13d 9h09m07s
system limits: memmax = unlimited; ulimit-n = 4122
maxsock = 4122; maxconn = 2000; maxpipes = 0
current conns = 706; current pipes = 0
Running tasks: 3/814
```

|           | Queue |        |        | Session rate |        |        | Sessions |         |               | Bytes         |                   |                 | Denied          |     | Errors |       |       | Warnings  |             | Server   |             |         |      |     |        |     | Thrtle |        |
|-----------|-------|--------|--------|--------------|--------|--------|----------|---------|---------------|---------------|-------------------|-----------------|-----------------|-----|--------|-------|-------|-----------|-------------|----------|-------------|---------|------|-----|--------|-----|--------|--------|
|           | Curr  | Max    | Limit  | Curr         | Max    | Limit  | Curr     | Max     | Limit         | Total         | LbTot             | In              | Out             | Req | Resp   | Req   | Conn  | Resp      | Retr        | Redis    | Status      | LastChk | Wght | Act | Bck    | Chk | Dwn    | Dwntme |
| Frontend  | 1 337 | 15 577 | 75 000 | 1 337        | 15 577 | 75 000 | 3 227    | 642 671 | 3 227         | 615 876       | 1 004             | 266 573 959     | 143 617 833 174 | 0   | 0      | 490   | 1 310 | 93344     | 4842        | 13d9h UP | L4OK in 0ms | 8       | 8    | 0   |        | 0   | 0s     | -      |
| index.net | 0     | 0      | -      | 183          | 3 714  | 8      | 329      | -       | 390 880 285   | 390 879 744   | 110 154 081 687   | 10 599 307 616  | 0               | 23  | 23     | 541   | 0     | 13d9h UP  | L4OK in 0ms | 1        | Y           | -       | 0    | 0   | 0s     | -   |        |        |
| index.net | 0     | 0      | -      | 204          | 2 594  | 8      | 251      | -       | 425 486 587   | 425 486 338   | 118 854 805 028   | 10 370 585 251  | 0               | 0   | 22     | 249   | 0     | 13d9h UP  | L4OK in 0ms | 1        | Y           | -       | 317  | 0   | 0s     | -   |        |        |
| index.net | 0     | 0      | -      | 178          | 2 511  | 8      | 478      | -       | 426 872 856   | 426 872 644   | 126 657 431 281   | 18 126 859 347  | 0               | 0   | 42     | 212   | 0     | 13d9h UP  | L4OK in 0ms | 1        | Y           | -       | 319  | 0   | 0s     | -   |        |        |
| index.net | 0     | 0      | -      | 167          | 2 512  | 14     | 356      | -       | 389 212 030   | 389 210 818   | 117 239 608 527   | 16 427 055 232  | 0               | 0   | 116    | 1212  | 490   | 13h23m UP | L4OK in 1ms | 1        | Y           | -       | 375  | 2   | 55m55s | -   |        |        |
| index.net | 0     | 0      | -      | 1976         |        |        |          | -       | 427 177 599   | 427 129 382   | 171 690 764 829   | 51 225 738 136  | 0               | 386 | 402    | 48217 | 2390  | 1h20m UP  | L4OK in 1ms | 1        | Y           | -       | 2875 | 15  | 32m56s | -   |        |        |
| index.net | 0     | 0      | -      | 591          |        |        |          | -       | 408 712 279   | 408 672 399   | 132 220 343 543   | 9 907 313 004   | 0               | 81  | 212    | 39881 | 1605  | 1h20m UP  | L4OK in 0ms | 1        | Y           | -       | 2804 | 15  | 33m20s | -   |        |        |
| index.net | 0     | 0      | -      | 107          | 4 080  | 7      | 494      | -       | 368 420 101   | 368 417 326   | 113 777 789 833   | 18 377 072 857  | 0               | 0   | 224    | 2775  | 357   | 13h23m UP | L4OK in 1ms | 1        | Y           | -       | 428  | 12  | 57m2s  | -   |        |        |
| Backend   | 0     | 0      | -      | 1 337        | 15 658 | 700    | 2 000    | 10 000  | 3 227 642 671 | 3 227 615 876 | 1 004 266 573 959 | 143 617 833 174 | 0               | 0   | 490    | 1 310 | 93344 | 4842      | 13d9h UP    |          | 8           | 8       | 0    |     | 0      | 0s  | -      |        |

- | ● And | Session rate |     | Sessions |     |       | Bytes |       | Denied |             | Errors    |                 |                | Warnings      |      | Server |      |       |        |         |          |             |     | Thrtle |     |     |        |     |   |
|-------|--------------|-----|----------|-----|-------|-------|-------|--------|-------------|-----------|-----------------|----------------|---------------|------|--------|------|-------|--------|---------|----------|-------------|-----|--------|-----|-----|--------|-----|---|
|       | Cur          | Max | Limit    | Cur | Max   | Limit | Total | LbTot  | In          | Out       | Req             | Resp           | Req           | Conn | Resp   | Retr | Redis | Status | LastChk | Wght     | Act         | Bck |        | Chk | Dwn | Dwntme |     |   |
|       |              |     |          |     |       |       |       |        |             |           |                 |                |               |      |        |      |       |        |         |          |             |     |        |     |     |        |     |   |
|       | Frontend     |     |          | 224 | 2 845 | -     | 5 988 | 10 000 | 428 176 566 |           | 162 370 658 994 | 94 269 636 319 | 0             | 0    | 0      |      |       | OPEN   |         |          |             |     |        |     |     |        |     |   |
|       | b.yandex.net | 0   | 0        | -   | 4     | 56    |       | 0 125  | -           | 8 563 567 | 8 563 546       | 3 247 497 190  | 1 890 113 708 |      | 0      | 0    | 2 939 | 21     | 0       | 13d9h UP | L4OK in 1ms | 1   | Y      | -   | 325 | 0      | 0s  | - |
|       | b.yandex.net | 0   | 0        | -   | 4     | 56    |       | 0 58   | -           | 8 563 552 | 8 563 546       | 3 247 075 836  | 1 889 958 287 |      | 0      | 0    | 30    | 6      | 0       | 13d9h UP | L4OK in 1ms | 1   | Y      | -   | 315 | 0      | 0s  | - |
|       | b.yandex.net | 0   | 0        | -   | 4     | 56    |       | 0 58   | -           | 8 563 557 | 8 563 546       | 3 248 067 982  | 1 890 091 759 |      | 0      | 0    | 612   | 11     | 0       | 13d9h UP | L4OK in 1ms | 1   | Y      | -   | 320 | 0      | 0s  | - |
|       | b.yandex.net | 0   | 0        | -   | 4     | 55    |       | 0 62   | -           | 8 563 555 | 8 563 546       | 3 246 684 450  | 1 890 208 385 |      | 0      | 0    | 700   | 9      | 0       | 13d9h UP | L4OK in 1ms | 1   | Y      | -   | 304 | 0      | 0s  | - |
|       | c.yandex.net | 0   | 0        | -   | 3     | 55    |       | 0 183  | -           | 8 563 762 | 8 563 476       | 3 247 048 585  | 1 882 670 226 |      | 0      | 1    | 9 409 | 286    | 69      | 5d23h UP | L4OK in 0ms | 1   | Y      | -   | 407 | 2      | 10s | - |
|       | c.yandex.net | 0   | 0        | -   | 4     | 55    |       | 0 120  | -           | 8 563 559 | 8 563 546       | 3 247 505 880  | 1 883 014 539 |      | 0      | 0    | 3 046 | 13     | 0       | 13d9h UP | L4OK in 1ms | 1   | Y      | -   | 399 | 0      | 0s  | - |
|       | y.yandex.net | 0   | 0        | -   | 4     | 55    |       | 0 138  | -           | 8 563 563 | 8 563 546       | 3 247 228 411  | 1 882 982 093 |      | 0      | 0    | 2 266 | 17     | 0       | 13d9h UP | L4OK in 0ms | 1   | Y      | -   | 383 | 0      | 0s  | - |
|       | y.yandex.net | 0   | 0        | -   | 4     | 55    |       | 0 167  | -           | 8 563 584 | 8 563 546       | 3 248 253 782  | 1 885 194 965 |      | 0      | 0    | 4 066 | 38     | 3       | 13d9h UP | L4OK in 0ms | 1   | Y      | -   | 383 | 0      | 0s  | - |
|       | y.yandex.net | 0   | 0        | -   | 4     | 55    |       | 0 131  | -           | 8 563 558 | 8 563 546       | 3 247 839 424  | 1 883 032 216 |      | 0      | 0    | 2 747 | 12     | 0       | 13d9h UP | L4OK in 0ms | 1   | Y      | -   | 389 | 0      | 0s  | - |
|       | y.yandex.net | 0   | 0        | -   | 4     | 55    |       | 0 129  | -           | 8 563 558 | 8 563 546       | 3 247 821 773  | 1 883 030 194 |      | 0      | 0    | 2 656 | 12     | 0       | 13d9h UP | L4OK in 0ms | 1   | Y      | -   | 365 | 0      | 0s  | - |
|       | y.yandex.net | 0   | 0        | -   | 3     | 55    |       | 0 187  | -           | 8 563 546 | 8 563 309       | 3 245 855 068  | 1 882 630 797 |      | 0      | 3    | 9 274 | 237    | 64      | 5d23h UP | L4OK in 0ms | 1   | Y      | -   | 385 | 2      | 16s | - |
|       | y.yandex.net | 0   | 0        | -   | 4     | 55    |       | 0 119  | -           | 8 563 554 | 8 563 546       | 3 248 408 747  | 1 883 015 640 |      | 0      | 0    | 3 182 | 8      | 0       | 13d9h UP | L4OK in 0ms | 1   | Y      | -   | 391 | 0      | 0s  | - |
|       | y.yandex.net | 0   | 0        | -   | 4     | 55    |       | 0 138  | -           | 8 563 565 | 8 563 546       | 3 248 436 364  | 1 883 040 180 |      | 0      | 0    | 2 448 | 19     | 0       | 13d9h UP | L4OK in 1ms | 1   | Y      | -   | 415 | 0      | 0s  | - |
|       | y.yandex.net | 0   | 0        | -   | 4     | 55    |       | 0 169  | -           | 8 563 589 | 8 563 546       | 3 248 345 846  | 1 885 248 735 |      | 0      | 1    | 4 242 | 43     | 5       | 13d9h UP | L4OK in 1ms | 1   | Y      | -   | 364 | 0      | 0s  | - |





Fail!

# Not this time ;(

- Our Zabbix RCE exploit doesn't work at Debian systems
- Yandex's zabbix was based on Debian or manually configured
- But we have come a long way and it is worth a look!



# We did not give up!

## **NEVER GIVE UP!**

- More exploits and vulns later
- Follow us at  
HITB2013AMS



???

@ONsec\_Lab [<http://lab.ONsec.ru>]

@d0znpp

d0znpp@onsec.ru

