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)

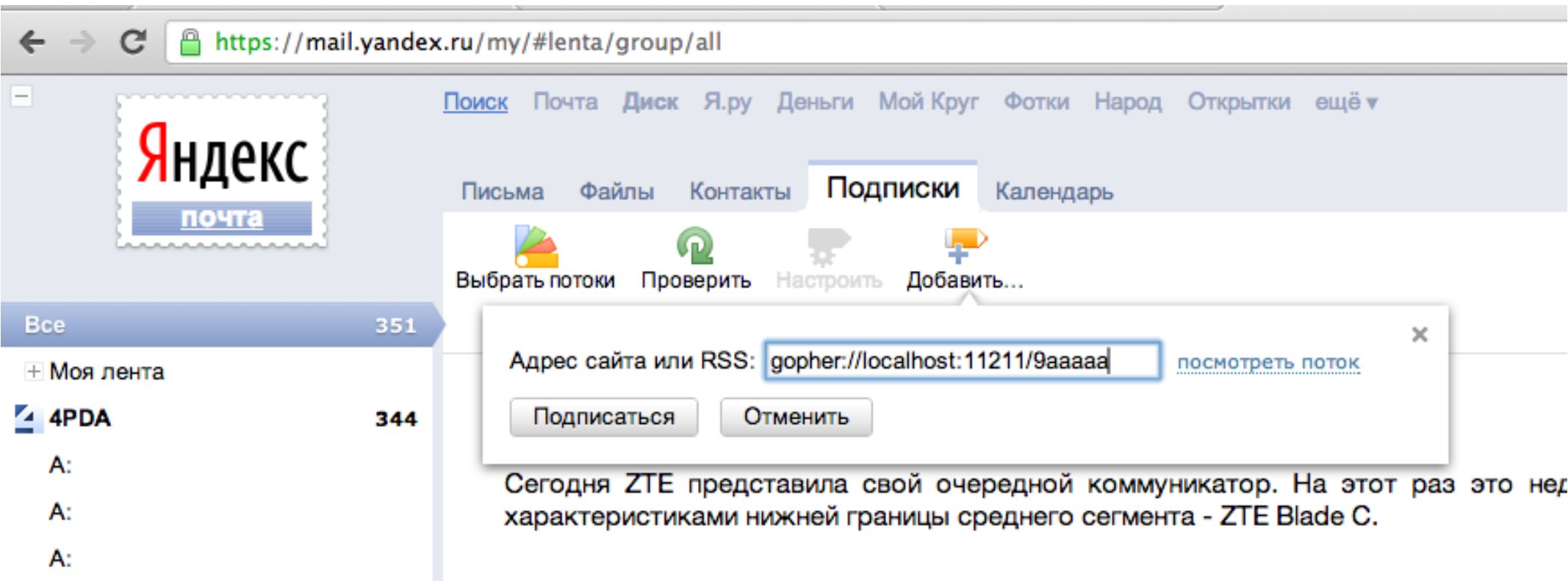
Memcached injection through SSRF

- All theory described at our ZeroNights report: www.slideshare.net/d0znpp/ssrf-attacks-and-sockets-smorgasbord-of-vulnerabilities
- Find possibility to write in sockets:

ANYPREFIX\nyoudata\nANYPOSTFIX

- Write it to localhost 11211 port - easy!

Memcached injection through SSRF



Nice "RCE" story: stages

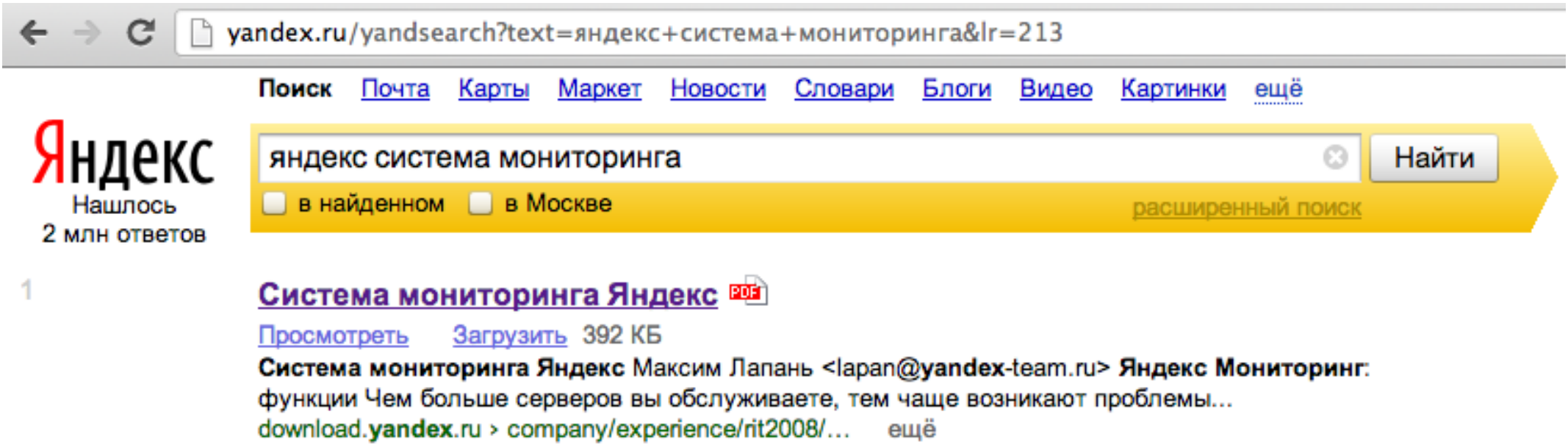
- Determine target
- Find information leaks
- Find vulns
- Find SSRF to exploit vulns
- Exploit vuln through SSRF

Determine target

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

Find information leaks

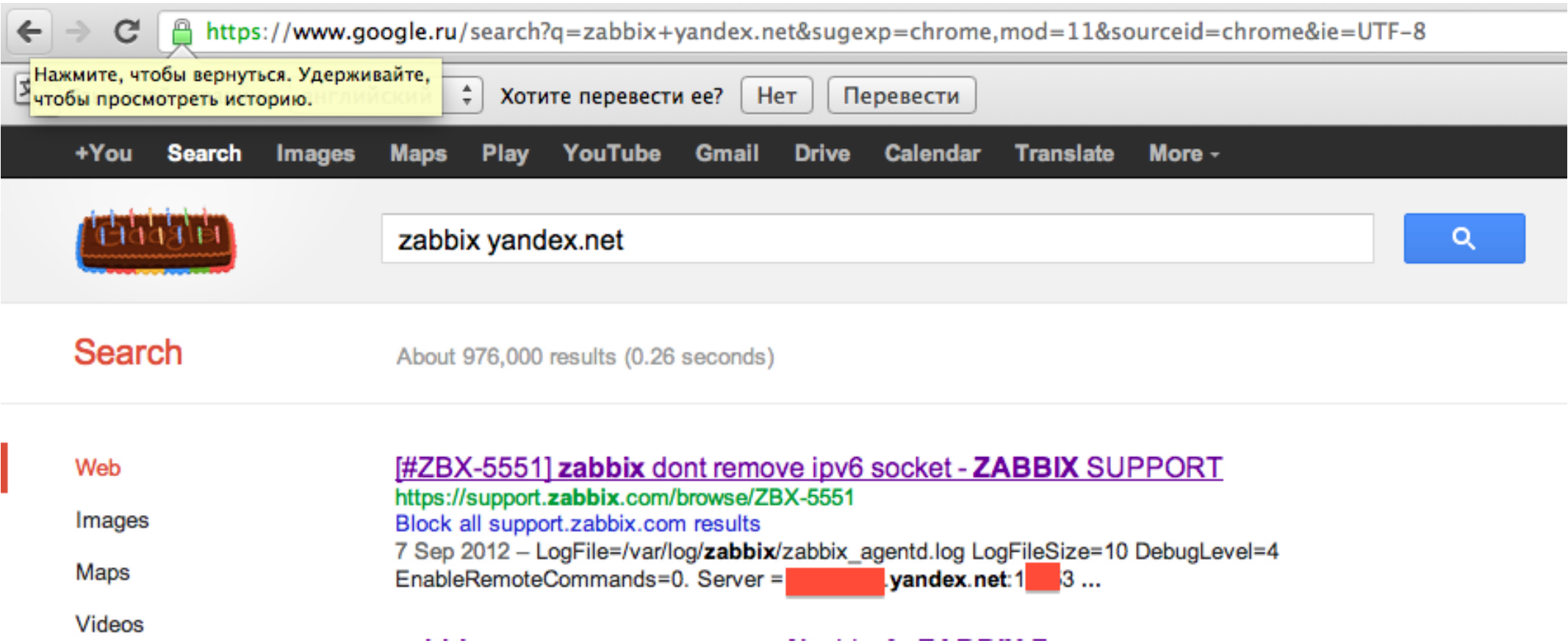
- Use Yandex to hack Yandex:



- This presentation contain info about Zabbix

Find information leaks

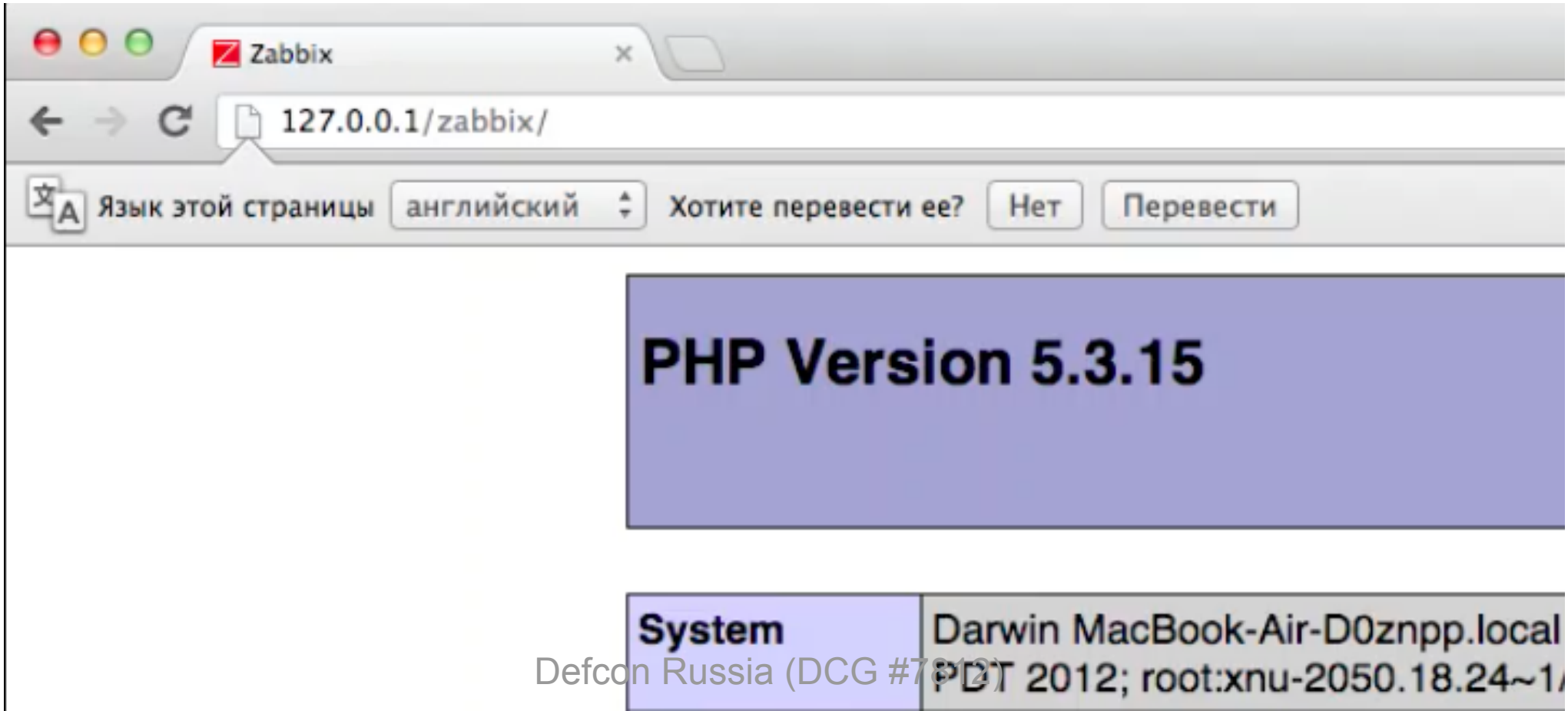
- Use Google to hack Yandex:



- This ticket contained intranet host of Zabbix in Yandex

Find vulns in Zabbix

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



Find SSRF and exploit it!

- SSRF attack from host which can establish connections to Zabbix host
- SSRF restrictions to make exploitation possible
- And...


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!

- More exploits and vulns later
- Follow us at HITB2013AMS

???

@ONsec_Lab [http://lab.ONsec.ru]
@d0znpp

d0znpp@onsec.ru