Offensive IDS

By **@asintsov**

For Russian Defcon Group

15/06/11

Who is an attacker?

© Tite Kubo/Shueisha, TV TOKYO, dentsu, Pierrot

Script Kiddies

Professionals

Fun

CC/Bank Accounts

Espionage

How they are doing it?

- SQL injection
- XSS/Steal sessions
- Client side vulns.
- e.t.c.

IDS/IPS

- Detect an attack
- Detect an attacker
- Prevent an attack
- e.t.c.

Detect an attacker?

- Web-Proxy
- TOR
- Socks
- Pwned hosts

Offensive?

- Bugs in C&C
  http://data.proidea.org.pl/confidence/8edycja/materialy/prezentacje/AndrzejDereszowski.pdf
- Botnet takeover
  Story from my life: RFI sploit->parse PHP->IRC login/pass
- Honey Tokens
- Social Engineering

Simple web attacks

- ‘ “ > < %00 ../ - everyone tries that 8)
- Trying to find admin.php
- Fast bruteforce, like admin:admin

Give to an attacker what he want

- Honey Token – create admin.php
- Make regexp on “admin” password

```
preg_match( "/^[\\\w\d\-\+]*\'\s+or\s+/i"  , $input)
```

- If trigger fires: SE attacks – java or activeX as “admin-panel-GUI”

Social Engineering

An attacker must believe that it is GUI

What we get?

- Info about an attacker’s workstation
- Local DNS settings
- Traceroute can show us attaker’s home (even if attacker run from VMware)
- We can control an attacker’s workstation

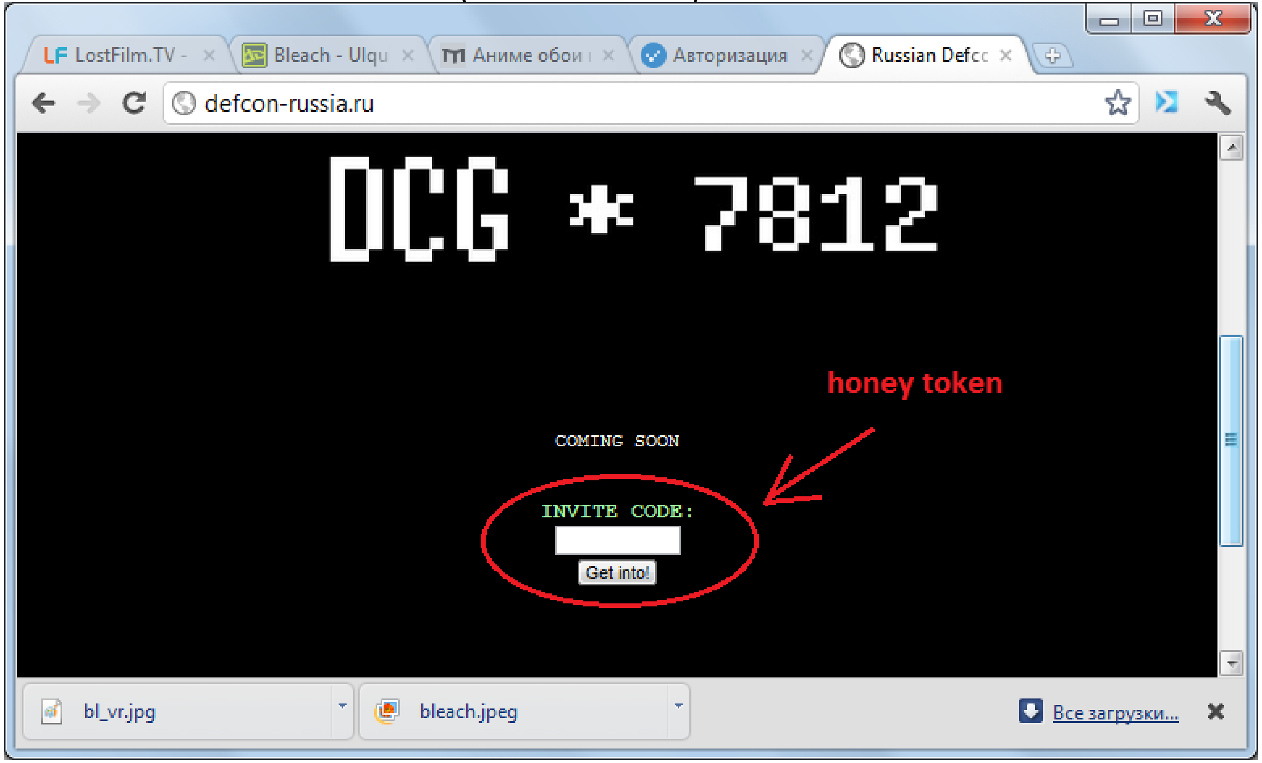
Defcon-Russia
INVITE CODE

P.S Harder– everyone suspect our plugin 8)

Quest, Contest, something fun, but not real GUI...

But it works!

(DNS bot inside)



Defcon-Russia web logs

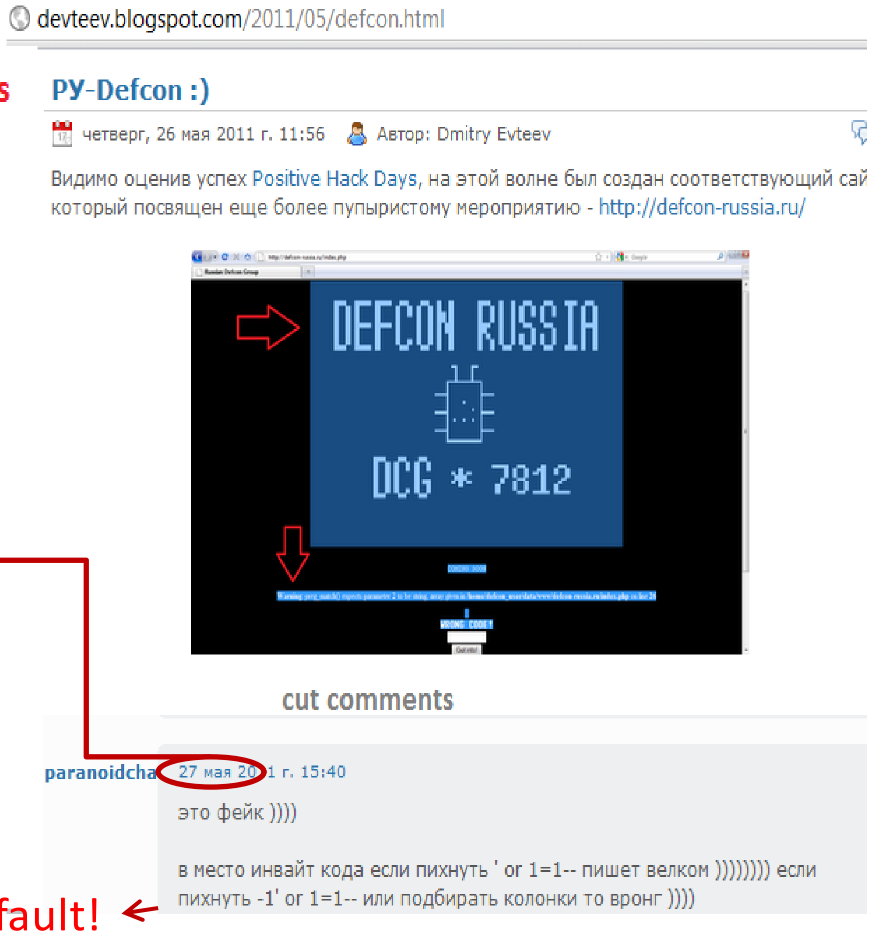
```
Thursday, May 26, 2011:87.245.151.90:[\' or 2=2-- 1 ]
Thursday, May 26, 2011:87.245.151.90:[\' or 2=1-- 1 ]
Thursday, May 26, 2011:87.245.151.90:[\' or ]
Thursday, May 26, 2011:87.245.151.90:[\' or 2=2]
Thursday, May 26, 2011:87.245.151.90:[\' or 2=1]
Thursday, May 26, 2011:213.239.195.202:[\' or 2=1]
Thursday, May 26, 2011:87.245.151.90:[\' or 2=]
Thursday, May 26, 2011:213.239.195.202:[\' or 2=]
Thursday, May 26, 2011:213.239.195.202:[\' or 2]
Thursday, May 26, 2011:213.239.195.202:[\' or ]
Thursday, May 26, 2011:87.245.151.90:[\' or ]
Thursday, May 26, 2011:87.245.151.90:[\' or sleep(20)]
Thursday, May 26, 2011:213.239.195.202:[\' or \"><script>alert()</script>]
Thursday, May 26, 2011:95.108.170.223:[\' or \'1\' = \'1]
Thursday, May 26, 2011:82.203.205.227:[\' or \'1\'=\'1DSECTEST]
Friday, May 27, 2011:80.70.234.113:[\' or \'1\'=\'1DSECTEST]
Friday, May 27, 2011:85.132.26.129:[\' or 1=1--]
Friday, May 27, 2011:85.132.26.129:[\' or 1=1--]
Friday, May 27, 2011:85.132.26.129:[\' or 1=1--]
Friday, May 27, 2011:85.132.26.129:[\' or 1=1--]
Friday, May 27, 2011:85.132.26.129:[\' or 1=1--]
Friday, May 27, 2011:85.132.26.129:[\' or 1=1--]
Friday, May 27, 2011:85.132.26.129:[\' or 1=1--]
Friday, May 27, 2011:81.177.34.197:[\' or 1=1--]
Friday, May 27, 2011:81.177.34.197:[\' or 1=1--]
Friday, May 27, 2011:81.177.34.197:[\' or 1=1--]
Friday, May 27, 2011:81.177.34.197:[\' or 1=1--]
Friday, May 27, 2011:81.177.34.197:[\' or 1=1--]
Friday, May 27, 2011:81.177.34.197:[\' or 1=1--]
Friday, May 27, 2011:195.68.165.235:[\' or 1=1--]
Friday, May 27, 2011:212.192.248.201:[\' or 1=1--]
```

Positive Technologies play with us....

Yandex too...

Boring...

Yes, bad SE... my fault!



devteev.blogspot.com/2011/05/defcon.html

РУ-Defcon :)

четверг, 26 мая 2011 г. 11:56 Автор: Dmitry Evteev

Видимо оценив успех Positive Hack Days, на этой волне был создан соответствующий сай который посвящен еще более пупыристому мероприятию - http://defcon-russia.ru/

cut comments

paranoidcha 27 мая 2011 г. 15:40

это фейк))))

в место инвайт кода если пихнуть ' or 1=1-- пишет велком))))))) если пихнуть -1' or 1=1-- или подбирать колонки то вронг))))

Defcon-Russia
Java logs

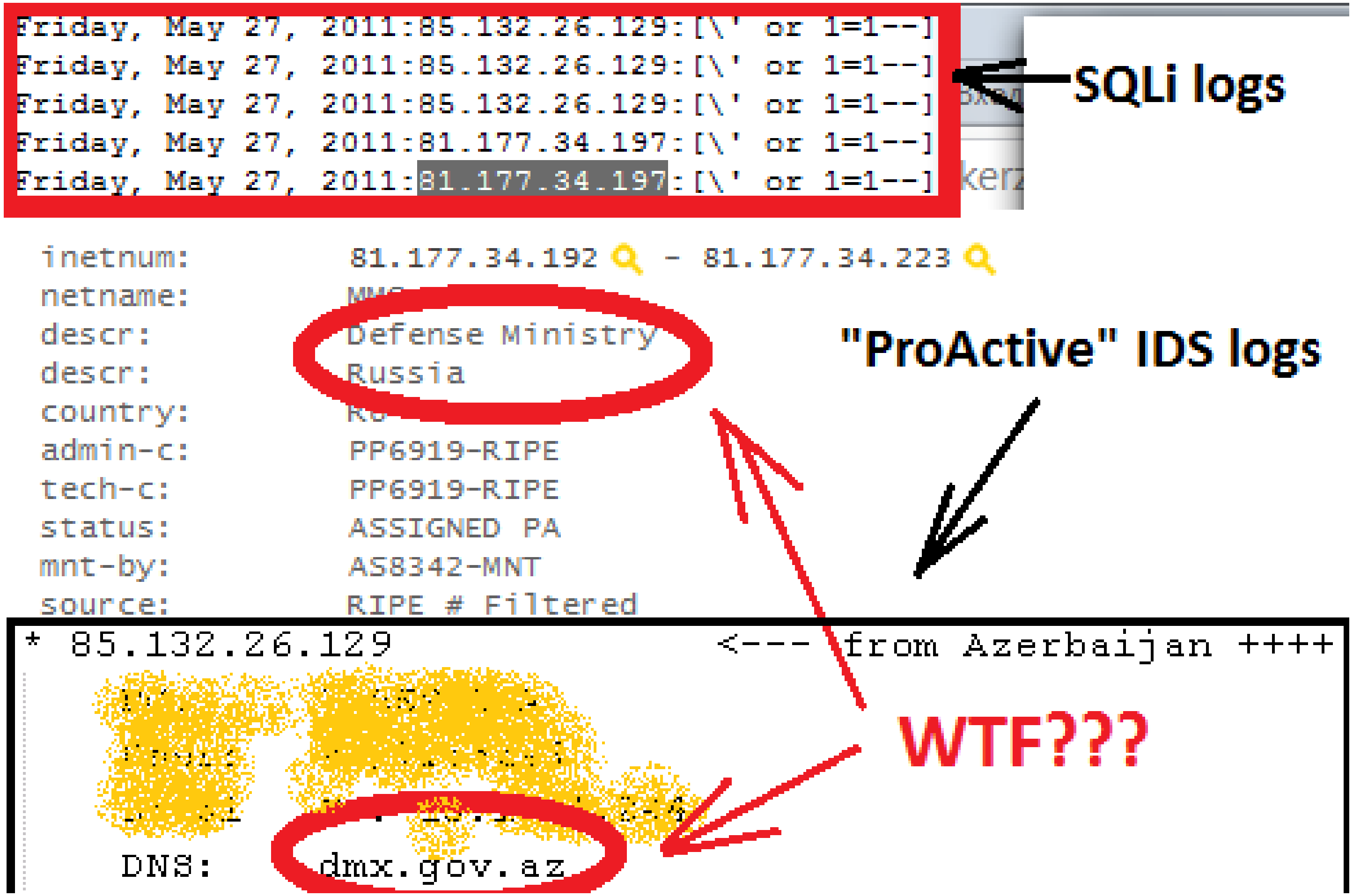
* 195.88.253.5
PC: \\BSODABLE <--- Dr. Web VMware
User: admin
Local IP: 192.168.239.1
Tracert: -> gw-virlab.i.drweb.ru(10.5.0.1) -> ge0-1-gw.dev.drweb.com(195.88.253.1) -> e0-1-1-ps.dev.drweb.com (84.204.76.97)

* 212.93.100.154 <--- Latvijas Mobilais Telefons SIA
PC: \\AMS-7CF3302AEC2 <--- looks like ax330d's VMware
User: Administrator
Local IP: 192.168.1.105

* 82.200.114.66
User: romashkin <--- **not Vmware**..he-he =)
DNS: olympus.f5net.com
Local IP: 192.168.167.55/192.168.170.1(VMware)/192.158.204.1

+ we have attackers DNS server IP! (we use reverse DNS channel)

Defcon-Russia
Government attacks



SQLi logs

```
Friday, May 27, 2011:85.132.26.129:[\' or 1=1--]
Friday, May 27, 2011:85.132.26.129:[\' or 1=1--]
Friday, May 27, 2011:85.132.26.129:[\' or 1=1--]
Friday, May 27, 2011:81.177.34.197:[\' or 1=1--]
Friday, May 27, 2011:81.177.34.197:[\' or 1=1--]
```

```
inetnum:        81.177.34.192 - 81.177.34.223
netname:        MMS
descr:          Defense Ministry
descr:          Russia
country:        RU
admin-c:        PP6919-RIPE
tech-c:         PP6919-RIPE
status:         ASSIGNED PA
mnt-by:         AS8342-MNT
source:         RIPE # Filtered
```

"ProActive" IDS logs

```
* 85.132.26.129                    <--- from Azerbaijan ++++
   [redacted]
   DNS:    dmx.gov.az
```

WTF???

Conclusion

- We can counterattack
- We can detect source of attack behind proxy (if SE works)
- We can do more, then just defend…
- Yeah … stupid slides with BLEACH, sorry 8)

Thx for pictures

- ***tobiee***
- **Albertos719**
- **Nova1Duke**
- **risi37**