Агрессия на стороне СОВ

@asintsov

Russian Defcon Group

15/06/11

Кто атакует?

Script Kiddies

Профи

По приколу
(«потому что могу»)

Боты, креды,
онлайн банкинг

Промышленный
шпионаж

Как они это делают?

- SQL injection
- XSS/Steal sessions
- Уязвимости клиента
- и.т.д.

IDS/IPS

- Определяем атаку
- Определяем атакующего
- Предотвращаем атаку
- и.т.д.

Определяем атакующего?

- Web-Proxy
- TOR
- Socks
- Промежуточные хосты

Будем грубее?

- Взлом C&C
  http://data.proidea.org.pl/confidence/8edycja/materialy/prezentacje/AndrzejDereszowski.pdf
- Перехват ботнета
  Забавный опыт: RFI sploit->parse PHP->IRC login/pass
- Honey Tokens
- Социальная инженерия

Простейшие атаки

- ‘ “ > < %00 ../ - все, кому не лень пробуют это
- Пытаются найти admin.php
- Пробуют примитивные пароли, типа admin:admin

Так дадим же атакующему чего он хочет…

- Honey Token – создадим admin.php
- Добавим regexp для пароля админа

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

- Если сработает: СИ атака – java или activeX, якобы это “admin-panel-GUI”

Социальная Инженерия

Главное, что бы атакующий поверил нам и нашему GUI

Что нам это может дать?

- Инфу о рабочей станции атакующего
- Информацию о ДНС
- Traceroute покажет нам откуда была атака (даже если атака с VMware)
- В принципе мы можем контролировать рабочую станцию атакующего

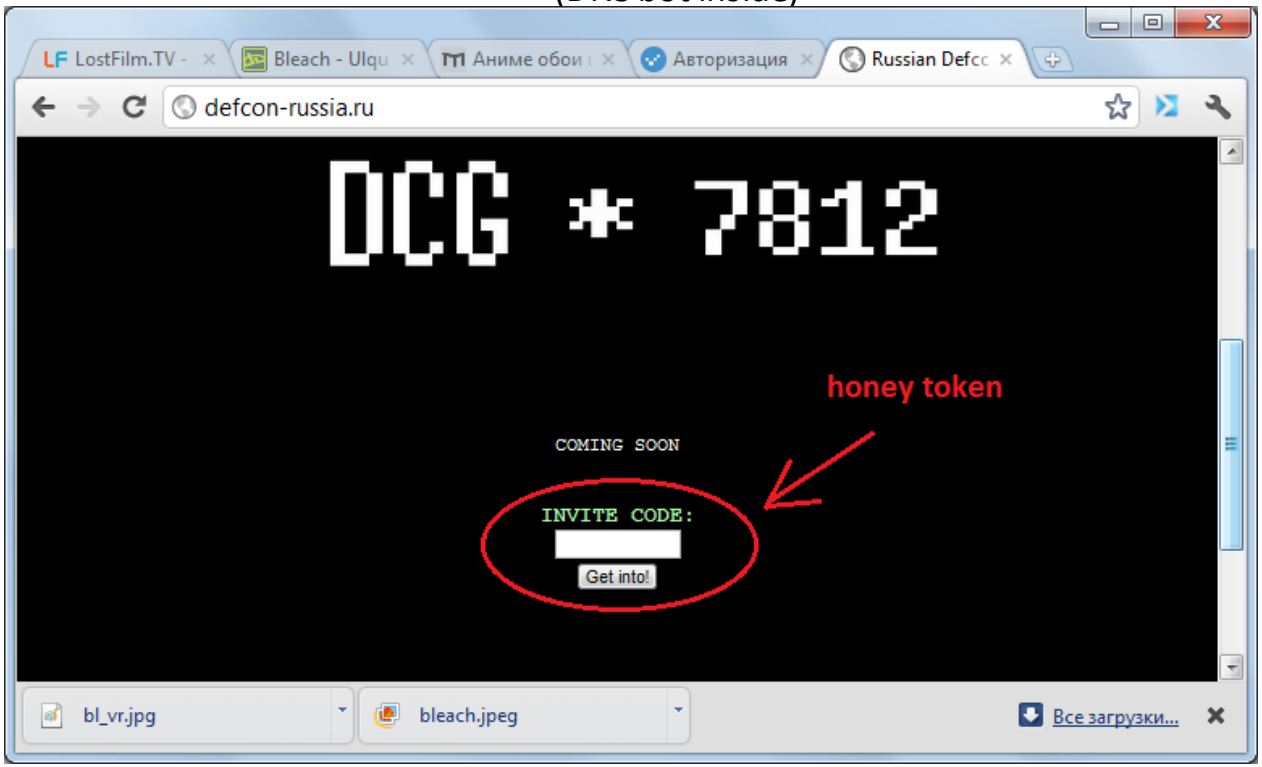
Defcon-Russia
INVITE CODE

P.S Немного сложнее, все с подозрением относятся к нашему ГУИ 8)

Quest, Contest, какой-то прикол, только не GUI…

Тем не менее это работает!

(DNS bot inside)



Defcon-Russia
web журнал

```
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>a[illegible]()</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:[\'[illegible]\'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, 2011:195.68.165.23[illegible]:[\' or 1=1--]
Friday, May 27, 2011:212.192.248.201:[\' or 1=1--]
```

Positive Technologies play with us....

Yandex too...

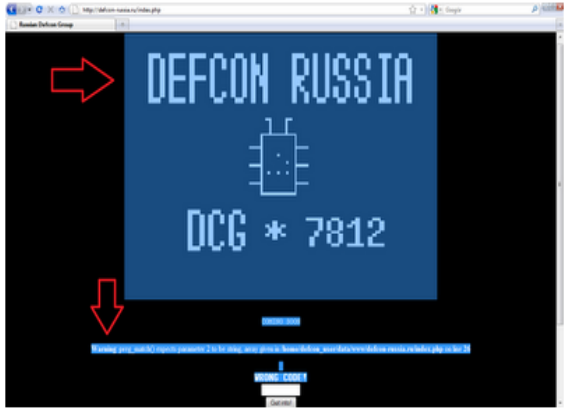
Boring...

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

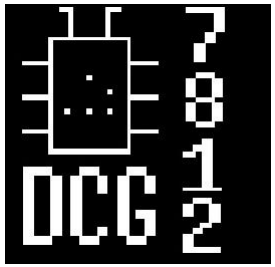
paranoidcha 27 мая 20[illegible]1 г. 15:40

это фейк))))

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

Yes, bad SE... my fault!

Defcon-Russia
Журнал “GUI”



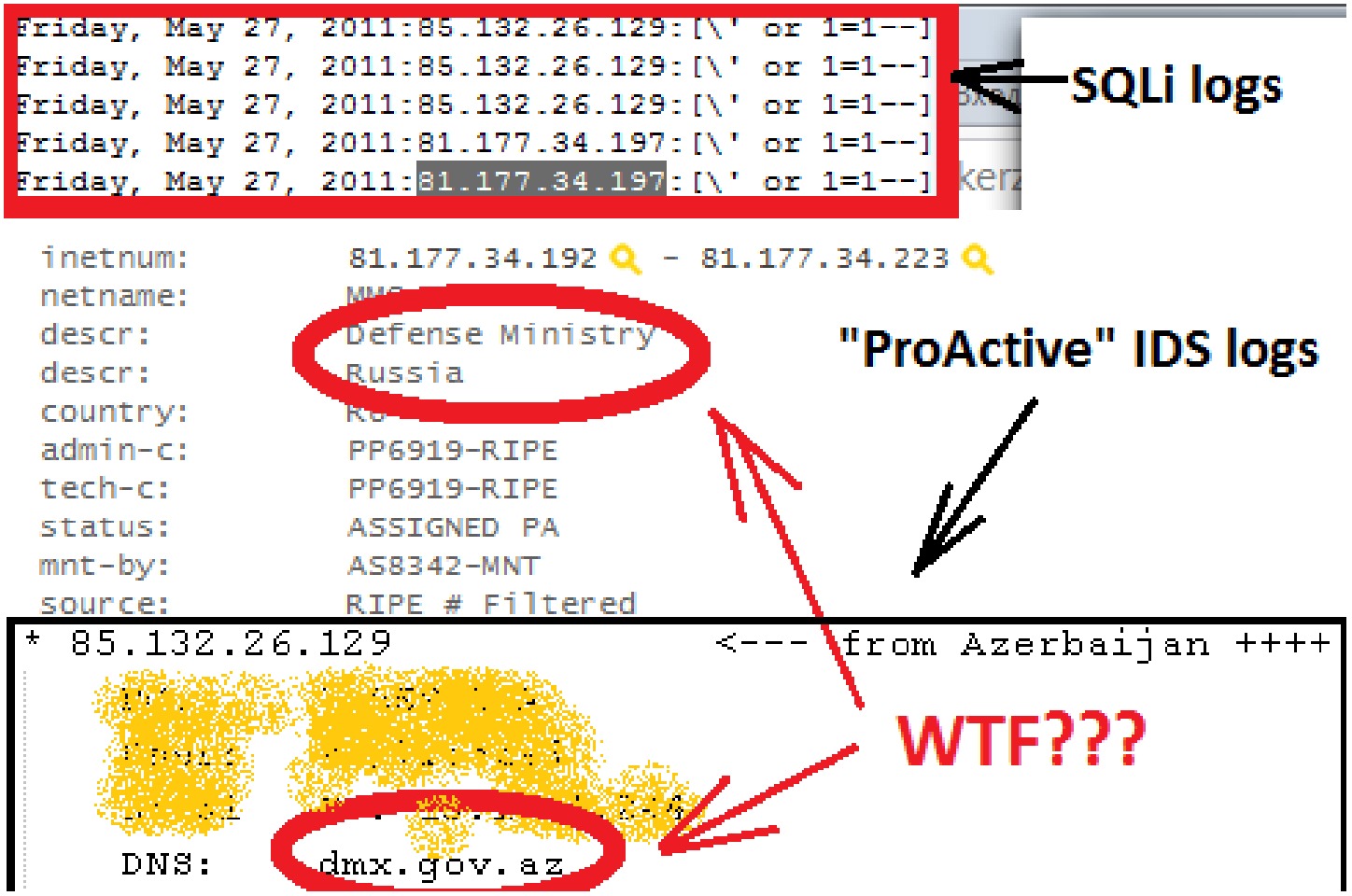
* 195.88.253.5
  PC: \\BSODABLE <--- Dr. Web VMware
  User: admin
  Local IP: 192.168.239.1
  Tracert: -> gw-virlab.i.drweb.ru(10.5.0.1) -> ge0-1-gw.dev.drweb.com(195.88.253.1) -> e0-1-1-ps.dev.drweb.com (84.204.76.97)

* 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

+ при использовании реверсивного DNS мы имеем дополнительную точку выхода – IP адрес сервера DNS

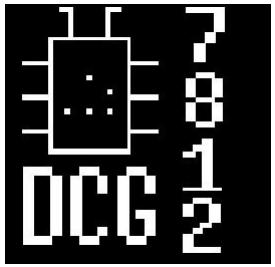
Defcon-Russia
Правительственные атаки



Выводы

- Мы можем контратаковать!
- Мы можем узнать об атакующем больше информации
- Мы можем гораздо больше, чем просто защищается…
- Да … слайды с картинками из BLEACH, извините 8)

Thx for pictures



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