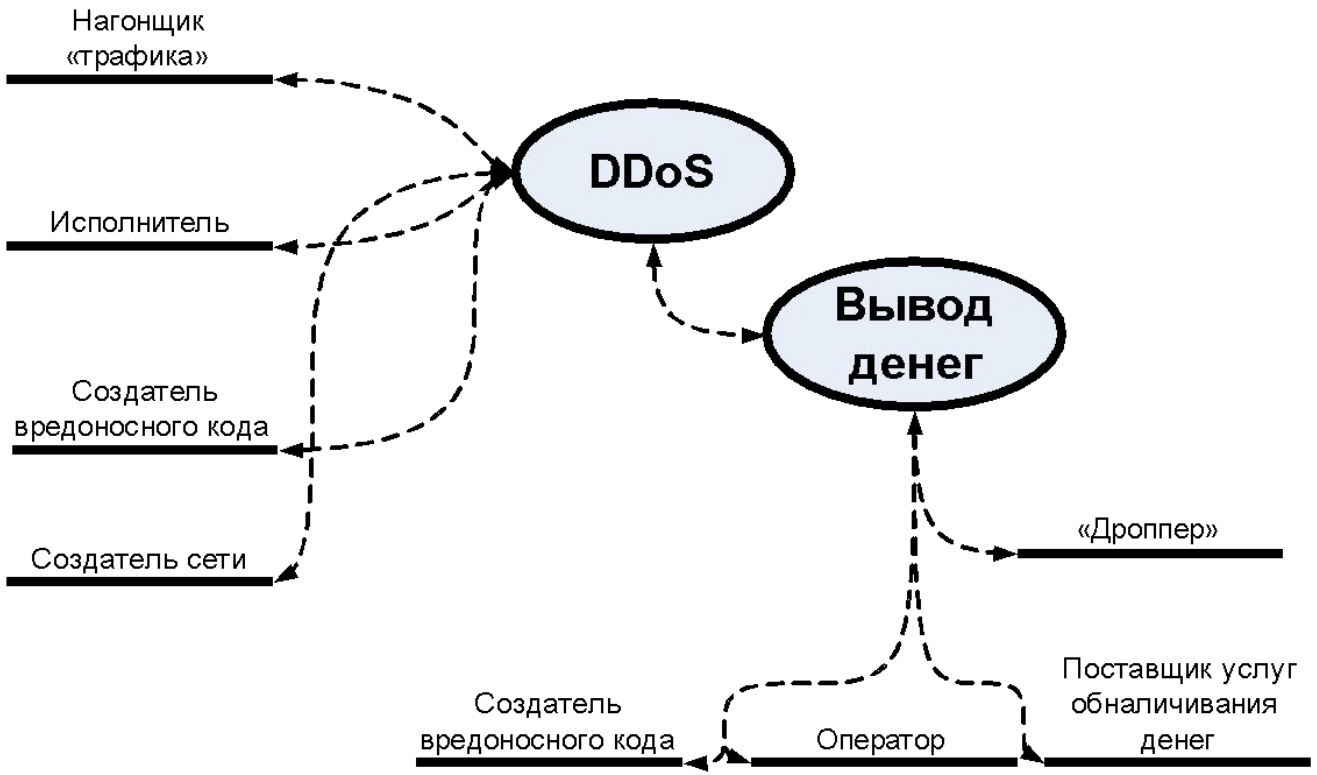
# Расследование DDoS атак.

# Расследование компьютерных инцидентов и преступлений в России.


Илья Сачков
*CISM*
Group-IB (Группа информационной безопасности)
sachkov@group-ib.ru

# Преступная группа

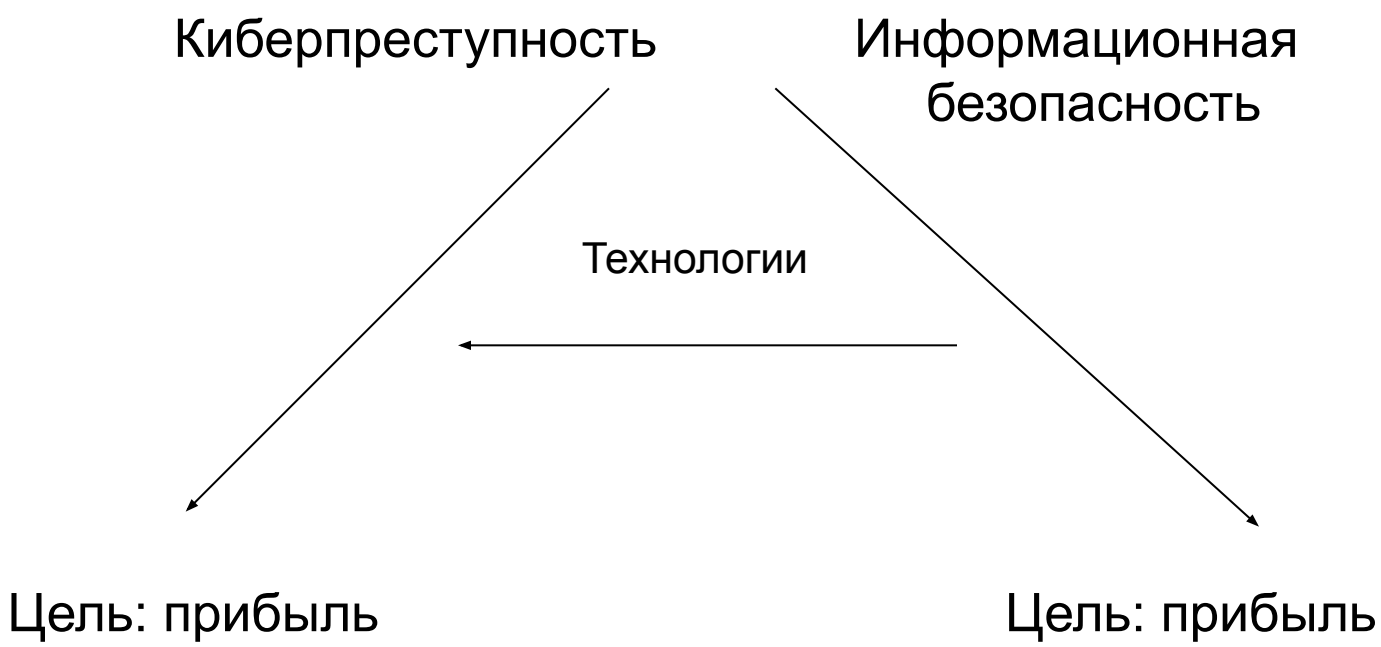


# Ответственность за нарушение ИБ

Отсутствие ответственности удешевляет стоимость нелегальных услуг и сводит работу информационной безопасности в гонку вооружений.

- 20$ стоимость заражения 1000 машин
- 200 – 500 Euro – DDoS атака до 20Гб (24 часа)

# Вектора развития



# Задачи расследования

1. Привлекать в ответственности преступников

Если этого не делать, то стоимость услуг будет далее дешеветь, а качество возрастать.

Как увеличить шансы:

1. Помогать правоохранительным органам
2. Обмениваться информацией (дела по одним и тем же людям лежат в разных подразделениях от разных заявителей)

**Нет идеальных преступлений – при желании можно найти все**

# Бот-сети. Тенденции 2009- 2010

1. Интеллектуальные боты

2. Появление ещё большого количества непрофессиональных бот сетей: с помощью конструкторов или специальных программ для их создания. Для создания и управления такой сетью не требуются специальные знания.

3. Профессиональные бот сети стали использовать передовые технологии для управления и обеспечения анонимности

4. Усиление партнерских бот-сетей («партнерки»).

# Бот-сети. Технологии

1. First come – установление патчей после заражения;

2. Port knocking – аутентификация;

3. Использование пиринговых сетей для управления бот-нетом. Skype, p2p и т.д.

4. Fast flux – уже почти стандарт.

5. Текстовые управляющие центры (социальные сети, блоги)

# DDoS атаки

В 2009 году основными сферами деятельности, подвергшимися DDoS атакам являлись:

- Банковские платежные системы
- Системы электронных платежей
- Предприятия электронной коммерции
- Средства массовой информации
- Телекоммуникационные компании

Расходы на атаку 100-500 евро в день.

# DDoS атаки

С прошлой недели и по текущий момент (с 15 апреля)

- медицинские клиники
- магазины автозапчастей
- оконные фабрики

# Используем возможности Honeynet

- Бот под контролем

*GET /main/rand/test.php?ver=0001id=151D4f12E2&cmd=0102 HTTP/1.0*
*Host: zlozlozlo.cn*
*HTTP/1.1 200 OK*
*Date: Tue, 26 Aug 2009 16:16:50 GMT*
*Server: Apache/2*
*X-Powered-By: PHP/5.0.11*
*Vary: Accept-Encoding,User-Agent*
*Content-Length: 17*
*Connection: close*
*Content-Type: text/html*

- Бот под контролем

*Host: zlozlozlo.cn*

IP: далеко.далеко.далеко.далеко

Делаем трассировку!

- В реальности все ближе

Tracert IP: далеко.далеко.далеко.далеко

*:7  11msk.datacentr.ru (120.209.15.202)  49.418 ms  49.416 ms  49.322 ms*
*8  77.91.231.212 (77.91.231.212)  49.440 ms  49.306 ms  49.822 ms*
*9  91.213.174.26 (196.213.174.26)  49.451 ms  49.545 ms  49.704 ms*
*7  te2.msk.dadadata.ru (155.239.10.202)  49.418 ms  49.416 ms  49.322 ms*
*8  77.91.231.212 (177.91.231.212)  49.440 ms  49.306 ms  49.822 ms*
*9  91.213.174.26 (99.213.174.26)  49.451 ms  49.545 ms  49.704 ms*
*7  tmsk.datacentr.ru (19.23.104.202)  49.418 ms  49.416 ms  49.322 ms*
*8  77.91.231.212 (177.191.21.212)  49.440 ms  49.306 ms  49.822 ms*
*9* далеко.далеко.далеко.далеко *(*далеко.далеко.далеко.далеко*)  49.451 ms  49.545 ms  49.704 ms*

## Преимущества:

- Быстро
- Бесплатно
- Если сервер в РФ расследование упрощается в разы
- Есть вредоносная программа(273 по старой практике)

## Недостатки:

- Не всегда работает (новые технологии ботнетов)
- Бота может не быть в Honeynet

- Смотрим схему

# Сбор доказательств

1. IP адреса (IP to IP с указанием времени)
2. Дамп трафика.
   *Не нужны 30 ГБ файлы. Нужен фрагмент до 100 Мб. Если трафик меняется – новый дамп.*
3. Делаем надпись на ресурсе «Сайт заблокирован» и нотариально снимаем копию – (скриптом)
4. Перед DDoS чаще всего идет сканирование ресурса, архитектуры сети. Снимаем логи с IDS.

*http://www.snort.org/snort-rules/?#rules*
*1 to 5 units - $499.00 each*
*6 or more units - $399.00 each*

5. Проверка информации в прессе/блогах и т.д.
6. Оформление служебной записки.
7. Расчет ущерба
8. Информация от Интернет-провайдера\хостинга

# Сбор доказательств на стороне ISP

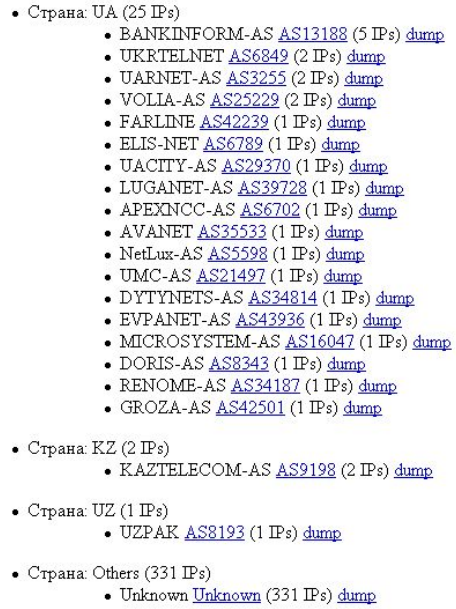
1. В договоре на оказание телекоммуникационных услуг добавьте пункт о Ваших требованиях по хранению и содержанию логов.
2. Оповещение со стороны ISP в случае атаки – в SLA

# Хорошие новости

В новых комментариях к УК РФ, выпущенных Верховным судом РФ – официальное признание создание бот сетей, а так же осуществления DDoS атак – преступлением.(272-273)

# Бот-сети. Наши меры

- Информация для IPS в режиме реального времени о нахождении бот-машин в их сетях.
- Распределенная кооперативная система для расследования DDoS атак и остановки
- StopDDOS.ru (Константин Тимашков)

# Бот-сети. Наши меры


Создание, поддержание, развитие  Российского сегмента Honeynet Project

Бесплатно устанавливаем HoneyPots, WatchDogs и другие кооперативные агенты для отслеживания и изучения бот-сетей.

Предоставление и обмен информацией на **некоммерческой** основе.

# Бот-сети и киберпреступность. Наши меры

RISSPA
be professional

Срочная бесплатная рассылка Group-IB & RISSPA:

- методы совершения компьютерных преступлений;
- сообщения с распределенных IDS систем о сетевых атаках и эпидемиях, о проводимых в данный момент DDoS атаках и информацию об активных бот-нета;
- данные с систем Honey Net о новых типах вредоносного ПО и способа его распространения.

Ассоциация RISSPA (Russian Information Systems Security Professional Association, www.risspa.ru)

# Бот-сети. Проблемы

1. Отсутствие в России работающих CERT'ов (Computer Emergency Response Team)

2. Отсутствие работающих международных соглашений и законодательства по борьбе с подобными явлениями.

3. Техническая безграмотность населения и простота заражения ПК вирусами. Стоимость заражения 1000 машин вирусами начинается от 20 долларов США.

4. Малое количество успешных уголовных дел из-за сложностей законодательства и правовых уловок, которыми пользуются злоумышленники и их адвокаты

# Мой любимый реальный пример

- Как Вы думаете, сколько зарабатывает создатель «средней» по технологии бот сети?

Please find total summary of your income for specific date or time period.
**RPU** — means average Revenue Per Unique.
**RPO** — means average Revenue Per Order.
Please select time period for report

○ Today ○ This week 01.01.2007
○ Yesterday ○ This month ● 17.01.2009 show

**Report for: 01.01.2007—17.01.2009**

| Date | Raw | Unique | RPU | RPO | Ratio | Sale | Pending | Profit | Refs | Total |
|---|---|---|---|---|---|---|---|---|---|---|
| 2009-01-17 | 10704 | 7989 | $0.01 | $36 | 1:2663 | 3 | 0 | $107.49 | $8.68 | $116.17 |
| 2009-01-16 | 5050 | 2613 | $0.32 | $49 | 1:154 | 17 | 1 | $827.47 | $16.59 | $844.06 |
| 2009-01-15 | 3145 | 1248 | $0.36 | $50 | 1:139 | 9 | 1 | $447.77 | $40.51 | $488.28 |
| 2009-01-14 | 8487 | 5422 | $0.1 | $45 | 1:452 | 12 | 2 | $540.36 | $10.86 | $551.22 |
| 2009-01-13 | 3078 | 1804 | $0.33 | $50 | 1:150 | 12 | 1 | $598.17 | $11.83 | $610 |
| 2009-01-12 | 4496 | 1411 | $0.34 | $60 | 1:176 | 8 | 2 | $479.68 | $74.98 | $554.66 |
| 2009-01-11 | 3134 | 957 | $0.51 | $61 | 1:120 | 8 | 2 | $489.41 | $21.48 | $510.89 |
| 2009-01-10 | 10225 | 1463 | $0.36 | $48 | 1:133 | 11 | 0 | $527.56 | $15.33 | $542.89 |
| 2009-01-09 | 5208 | 2500 | $0.5 | $63 | 1:125 | 20 | 3 | $1262.32 | $130.32 | $1392.64 |
| 2009-01-08 | 37959 | 5324 | $0.17 | $56 | 1:333 | 16 | 4 | $888.81 | $40.44 | $929.25 |
| 2009-01-07 | 19061 | 5316 | $0.21 | $46 | 1:213 | 25 | 5 | $1142.92 | $107.83 | $1250.75 |
| 2009-01-06 | 59602 | 11061 | $0.09 | $41 | 1:461 | 24 | 5 | $991.72 | $62.37 | $1054.09 |
| 2009-01-05 | 18687 | 10446 | $0.12 | $76 | 1:653 | 16 | 1 | $1218.1 | $57.3 | $1275.4 |

# Реальный пример

- 1 733 492 $ за 1.5 года

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 2007-07-06 | 10670 | 4645 | $1.16 | $41 | 1:35 | 132 | 0 | $5377.56 | $418.56 | $5796.12 |
| 2007-07-05 | 12550 | 5222 | $0.83 | $37 | 1:44 | 118 | 0 | $4331.42 | $379.23 | $4710.65 |
| 2007-07-04 | 5851 | 2385 | $0.91 | $34 | 1:37 | 64 | 0 | $2175.91 | $311.24 | $2487.15 |
| 2007-07-03 | 3870 | 1628 | $0.88 | $29 | 1:33 | 50 | 0 | $1440.75 | $519.3 | $1960.05 |
| 2007-07-02 | 1814 | 955 | $1.88 | $43 | 1:23 | 42 | 0 | $1793.96 | $347.92 | $2141.88 |
| 2007-07-01 | 1593 | 850 | $1.17 | $43 | 1:37 | 23 | 0 | $996.56 | $140.33 | $1136.89 |
| 2007-06-30 | 1661 | 910 | $3.94 | $38 | 1:10 | 94 | 0 | $3582.42 | $482.99 | $4065.41 |
| 2007-06-29 | 1951 | 949 | $7.26 | $39 | 1:5 | 175 | 0 | $6893.41 | $816.3 | $7709.71 |
| 2007-06-28 | 1500 | 789 | $4.36 | $45 | 1:10 | 76 | 0 | $3443.09 | $425.6 | $3868.69 |
| 2007-06-27 | 3050 | 1703 | $0.94 | $42 | 1:45 | 38 | 0 | $1604.47 | $274.16 | $1878.63 |
| 2007-06-26 | 3918 | 2175 | $0.52 | $34 | 1:66 | 33 | 0 | $1134.23 | $174.86 | $1309.09 |
| 2007-06-25 | 4263 | 2472 | $0.74 | $45 | 1:60 | 41 | 0 | $1826.93 | $109.1 | $1936.03 |
| Total | | 148111 | 98914 | 9118 | $0.18 | $45 | 1:257 | 3564399 | $1604494.72 | $128997.71 | $1733492.43 |

?


Илья Сачков
CISM
Группа информационной безопасности

sachkov@group-ib.ru
www.group-ib.ru