

Расследование компьютерных инцидентов и преступлений в России

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



- Цель нарушения информационной безопасности – получение прибыли. Большой прибыли.
-

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

Yesterday
 This month

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	1:266	33	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	

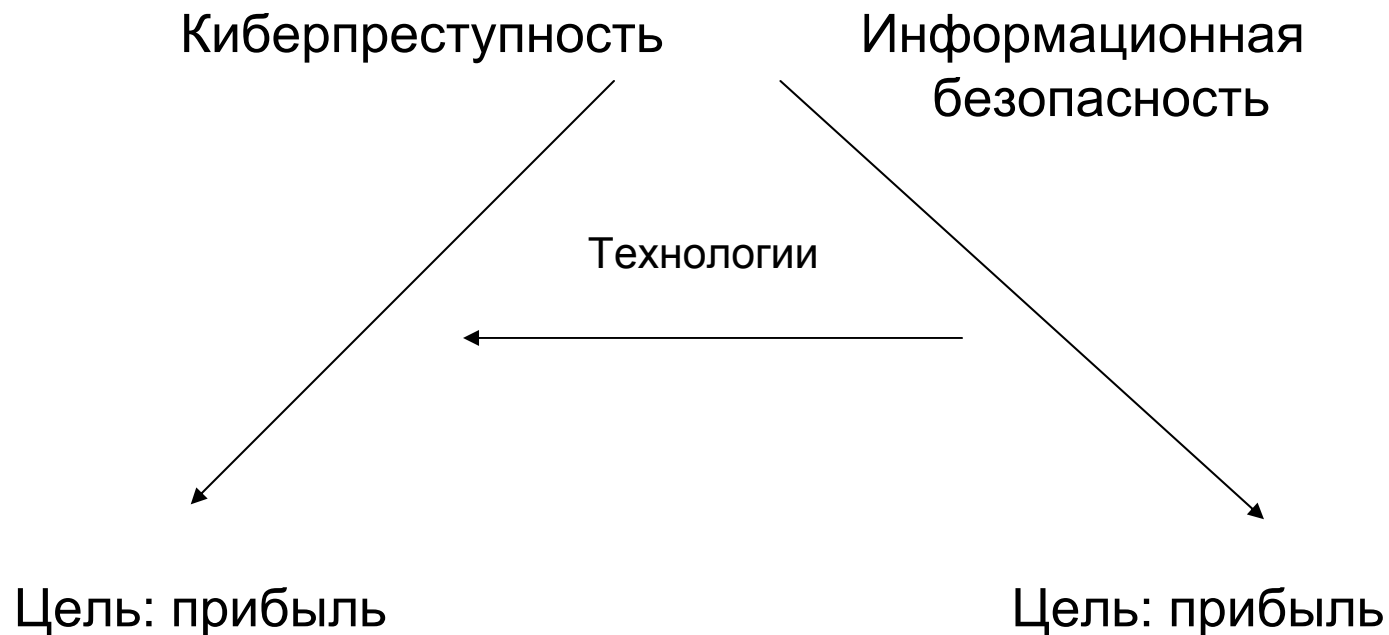
Реальный пример

- 1 733 492 \$ за 1.5 года

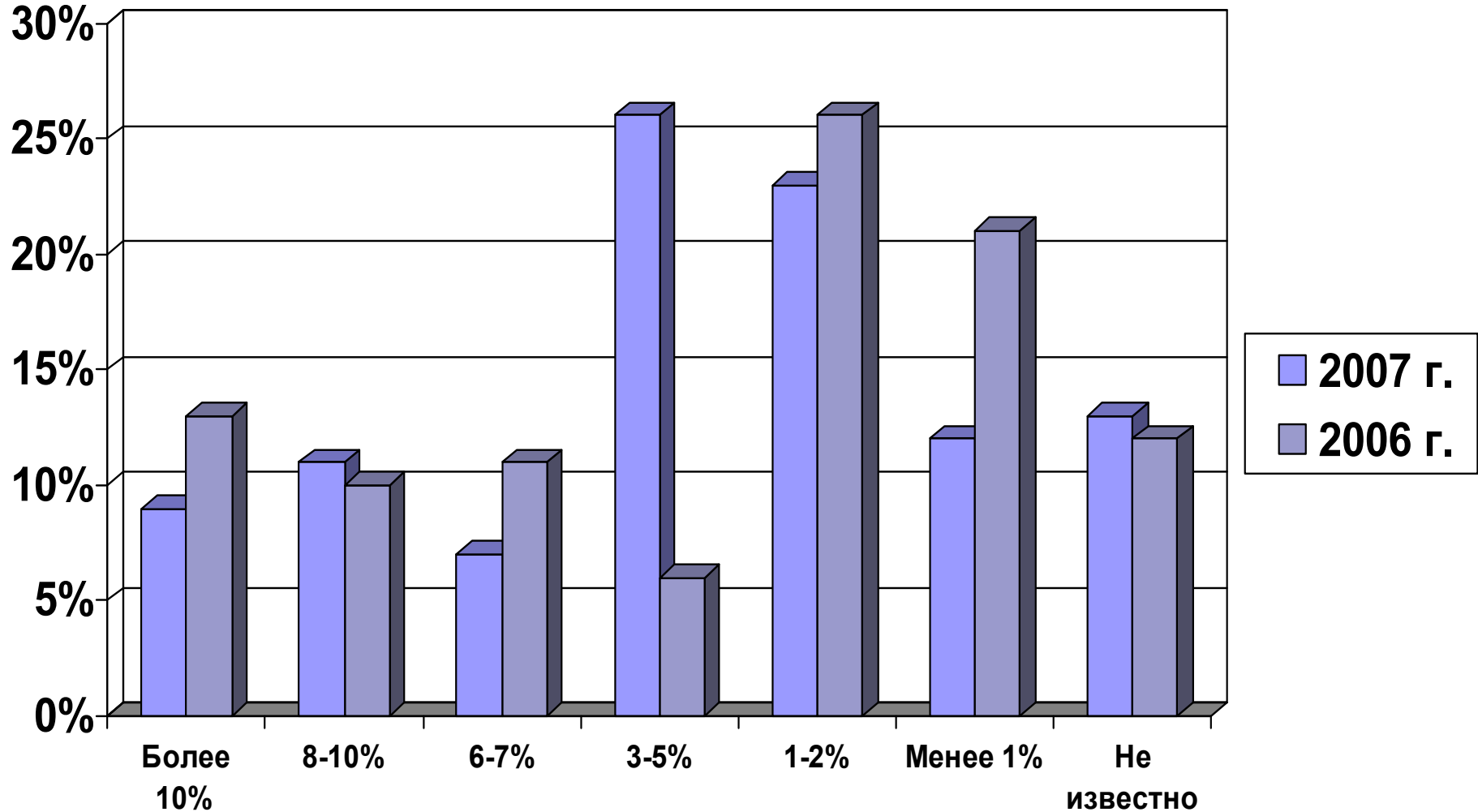
2007-07-06	10670	4645	\$1.16	\$41	1:35	132	0	\$5377.56	\$418.56	\$5796.12
2007-07-05	12550	5222	\$0.83	\$37	1:44	118	0	\$4331.42	\$379.23	\$4710.65
2007-07-04	5851	2385	\$0.91	\$34	1:37	64	0	\$2175.91	\$311.24	\$2487.15
2007-07-03	3870	1628	\$0.88	\$29	1:33	50	0	\$1440.75	\$519.3	\$1960.05
2007-07-02	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	148111989149118	\$0.18	\$45	1:257	3564399			\$1604494.72	\$128997.71	\$1733492.43

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

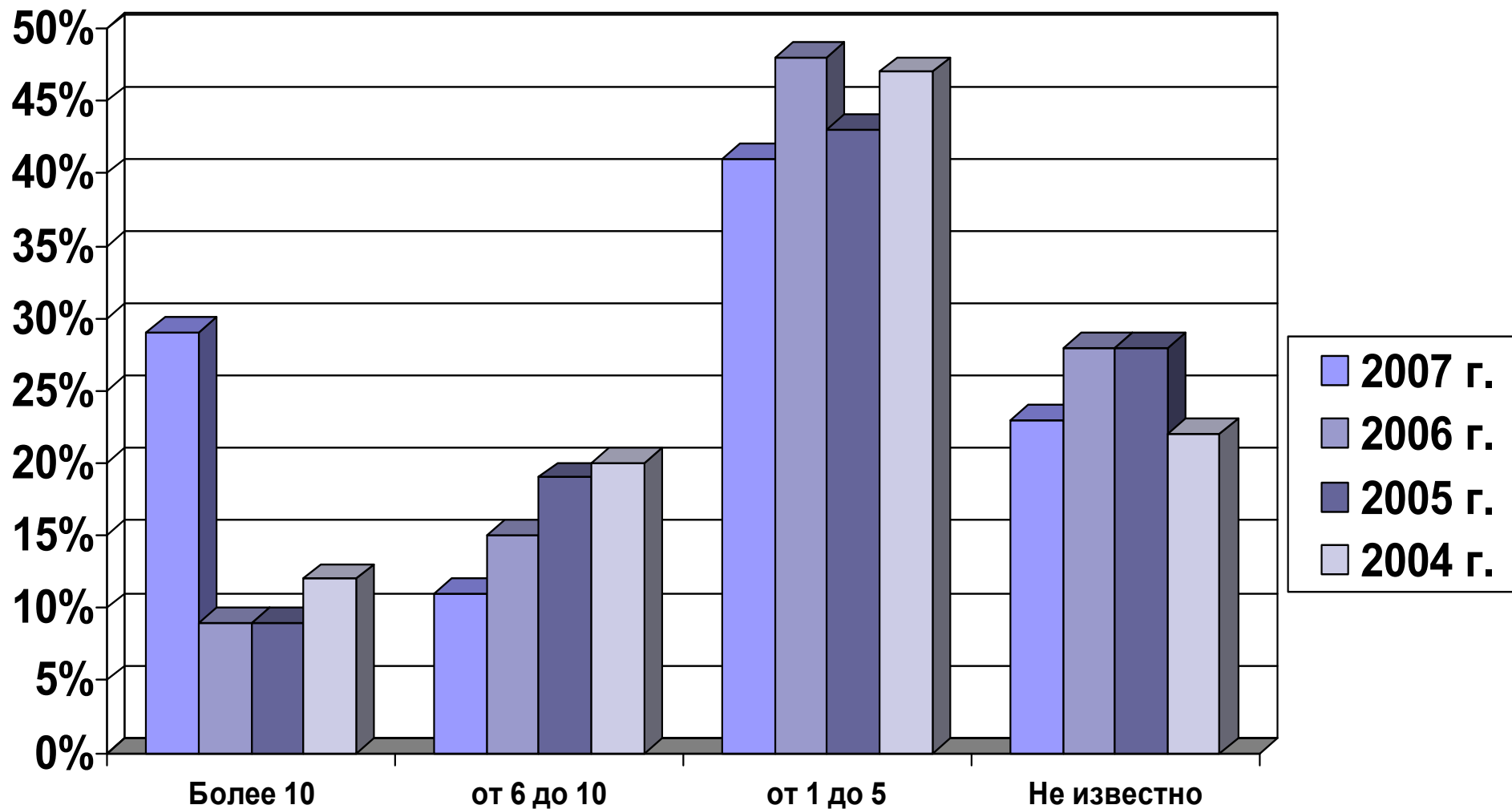
- 20\$ стоимость заражения 1000 машин
- 200 – 500 Euro – DDoS атака до 20Гб (24 часа)



Процент ИТ бюджета, который тратится на информационную безопасность



Как много инцидентов произошло у вас в компании за последний год?



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

DDoS атаки: реагирование и расследование

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



1. Укрупнение.
2. Децентрализация. Управляющие центры переносятся в «абузоустойчивые» страны и децентрализуются. Многоступенчатость управляющих центров.
3. Появление большого количества непрофессиональных бот сетей: с помощью конструкторов или специальных программ для их создания. Для создания и управления такой сетью не требуются специальные знания.
4. Профессиональные бот сети стали использовать передовые технологии для управления и обеспечения анонимности
5. Появления партнерских бот-сетей («партнерки»).

1. First come – установка патчей после заражения;
2. Port knocking – аутентификация;
3. Использование пиринговых сетей для управления бот-нетом. Skype, torrent и т.д.
4. Fast flux - назначение любому полнофункциональному доменному имени множества IP-адресов. Переключение между ними в потоке происходит с обескураживающей быстротой, при этом используется комбинация циклического набора IP-адресов и очень маленького значения TTL для каждой отдельной записи в DNS. Новый набор IP-адресов именам хостов может назначаться с периодичностью в три минуты.
5. Текстовые управляющие центры (социальные сети, блоги)

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

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.

Задачи:

- Минимизация потерь
- Восстановление сервиса
- Сбор доказательств

Что важнее? – решать оценке рисков

Но задачи должны выполняться параллельно.

DDoS атака: минимизация потерь

DDoS – не просто так.

- Постараться быстро ответить на вопрос:

Почему идет атака?

Как на ней зарабатывают?

Это поможет определить цель реальных действий.

1. Если Вы **Банк** – проверьте платежки!!!
90% DDoS на Российские банки за последние 3 месяца (за 12 месяцев 70%) – прикрытие по выводу денег со счетов клиента.
 - Авторизация по телефону
 - Проверка крупных сумм
 - Вывод на «физиков»
 - Антифрод решения - если есть деньги
 - Проверка IP, времени - если нет денег
2. **Клиент с украденными ключами:** не портить доказательства, заблокировать ключи в других банках.

Оперативная:

1. Перенаправление трафика в распределенную сеть (а-зоны, клипаги) (20 минут)
2. Защита на ISP (не всегда эффективна)

Защита на Вашей стороне – работает только от самых самых простых атак.

- 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
```

Останавливаем её за 20 минут. Неклассический способ

- 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
```

Abuse / Spam house / CERT

Блокируем/просим писать дампы

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

- Бота **нет** в Honey**net**
 1. Делаем выборку по атакующим IP адресам (не работает со «заспуфленными»)
 2. Смотрим ближайших ботов по ISP.
 3. Просим «помочь» ISP (используя рычаги)

Сбор доказательств

1. IP адреса (IP to IP с указанием времени)
2. Дамп трафика.
Не нужны 30 ГБ файлы. Нужен фрагмент. Если трафик меняется – новый дамп.
3. Делаем надпись на ресурсе «Сайт заблокирован» и нотариально снимаем копию

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*

4. В случае увода денег: Логи у клиента по вредоносному ПО – независимая экспертиза. Откуда отправили платеж?
5. Проверка информации в прессе/блогах и т.д.
6. Оформление служебной записки.

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

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)

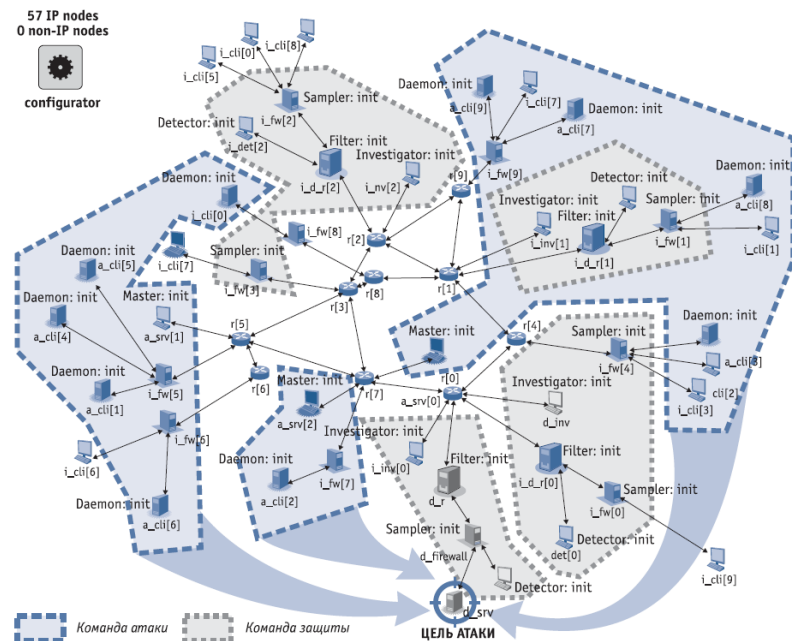
http://stopddos.ru/current/

- Страна: ru (48 IPs)
 - BEE-AS [AS16345](#) (5 IPs) [dump](#)
 - Unknown [Unknown](#) (4 IPs) [dump](#)
 - ROSTOV-TELEGRAF-AS [AS21479](#) (3 IPs) [dump](#)
 - COMCOR-AS [AS8732](#) (2 IPs) [dump](#)
 - NTK [AS31200](#) (2 IPs) [dump](#)
 - RIALCOM-AS [AS34456](#) (2 IPs) [dump](#)
 - Fiord-AS [AS28917](#) (2 IPs) [dump](#)
 - COMSTAR [AS8359](#) (2 IPs) [dump](#)
 - CIFRA-AS [AS41025](#) (2 IPs) [dump](#)
 - EXTREME-AS [AS39709](#) (1 IP) [dump](#)
 - STC-AS [AS25490](#) (1 IP) [dump](#)
 - ZTELECOM-AS [AS41733](#) (1 IP) [dump](#)
 - MF-NWGSIM-AS [AS31213](#) (1 IP) [dump](#)
 - RU-CTSND-AS [AS6767](#) (1 IP) [dump](#)
 - HOMELINK [AS39618](#) (1 IP) [dump](#)
 - MAconnet [AS8470](#) (1 IP) [dump](#)
 - SEVEREN-TELECOM [AS24729](#) (1 IP) [dump](#)
 - BWCOJSC-AS [AS41592](#) (1 IP) [dump](#)
 - URAL [AS5563](#) (1 IP) [dump](#)
 - TRT-AS [AS38951](#) (1 IP) [dump](#)
 - INFOLINE-AS [AS8416](#) (1 IP) [dump](#)
 - SIBIRTELECOM-AS [AS41440](#) (1 IP) [dump](#)
 - ASN-TVT [AS29194](#) (1 IP) [dump](#)
 - magistraly-ru [AS43970](#) (1 IP) [dump](#)
 - CORBINA-AS [AS8402](#) (1 IP) [dump](#)
 - LEALTA-AS [AS41275](#) (1 IP) [dump](#)
 - BTL-AS [AS43687](#) (1 IP) [dump](#)
 - SOVAM-AS [AS2216](#) (1 IP) [dump](#)
 - ROSTELECOM-AS [AS12389](#) (1 IP) [dump](#)
 - TATTELECOM-AS [AS28840](#) (1 IP) [dump](#)
 - ASTRARU-AS [AS42268](#) (1 IP) [dump](#)
 - UNNET-AS [AS31323](#) (1 IP) [dump](#)
 - RTCOMM-AS [AS8342](#) (1 IP) [dump](#)

- Страна: UA (25 IPs)
 - BANKINFORM-AS [AS13188](#) (5 IPs) [dump](#)
 - UKRTELNET [AS6849](#) (2 IPs) [dump](#)
 - UARNET-AS [AS3255](#) (2 IPs) [dump](#)
 - VOLIA-AS [AS25229](#) (2 IPs) [dump](#)
 - FARLINE [AS42239](#) (1 IP) [dump](#)
 - ELIS-NET [AS6789](#) (1 IP) [dump](#)
 - UACITY-AS [AS29370](#) (1 IP) [dump](#)
 - LUGANET-AS [AS39728](#) (1 IP) [dump](#)
 - APEXNCC-AS [AS6702](#) (1 IP) [dump](#)
 - AVANET [AS35533](#) (1 IP) [dump](#)
 - NetLux-AS [AS5598](#) (1 IP) [dump](#)
 - UMC-AS [AS21497](#) (1 IP) [dump](#)
 - DYTNETS-AS [AS34814](#) (1 IP) [dump](#)
 - EVPANET-AS [AS43936](#) (1 IP) [dump](#)
 - MICROSYSTEM-AS [AS16047](#) (1 IP) [dump](#)
 - DORIS-AS [AS8343](#) (1 IP) [dump](#)
 - RENOME-AS [AS34187](#) (1 IP) [dump](#)
 - GROZA-AS [AS42501](#) (1 IP) [dump](#)

- Страна: KZ (2 IPs)
 - KAZTELECOM-AS [AS9198](#) (2 IPs) [dump](#)
- Страна: UZ (1 IP)
 - UZPAK [AS8193](#) (1 IP) [dump](#)
- Страна: Others (331 IPs)
 - Unknown [Unknown](#) (331 IPs) [dump](#)

• Страна: UA (25 IPs)





Russian HoneyNet Project

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.



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)

?

Илья Сачков
CISM
Группа информационной безопасности

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

