Botnet

Суворов И.Б. ВМИ-456

Содержание

1. Определение ботнета
2. Немного истории
3. Архитектура ботнет сетей и способы управления
4. Самые известные ботнеты
5. Примеры ботнетов и способов борьбы с ними.

Опеределение Ботнета

Ботнет представляет собой совокупность систем, зараженных вредоносным кодом и управляемых централизованно.

Ботмастер выгуливает свой ботнет.

Почему они существуют?

- Уязвимости ПО
- Слабые методы защиты данных юзеров
- Сложность обнаружения создателя
- Огромная прибыль
- Распределенные вычисления
- Интерес

Почему они существуют?

- Уязвимости ПО:

Существует огромное множество различных уязвимостей, которые с большим удовольствием используют злоумышленники.

Почему они существуют?

- Слабые методы защиты данных юзеров

Почему они существуют?

- Огромная прибыль

$14 000 теряет средняя российская компания от одной атаки хакеров.

Почему они существуют?

- Распределенные вычисления

База в 40000 IP адресов позволяет взломать брутфорсом даже самый защищенный пароль.

Почему они существуют?

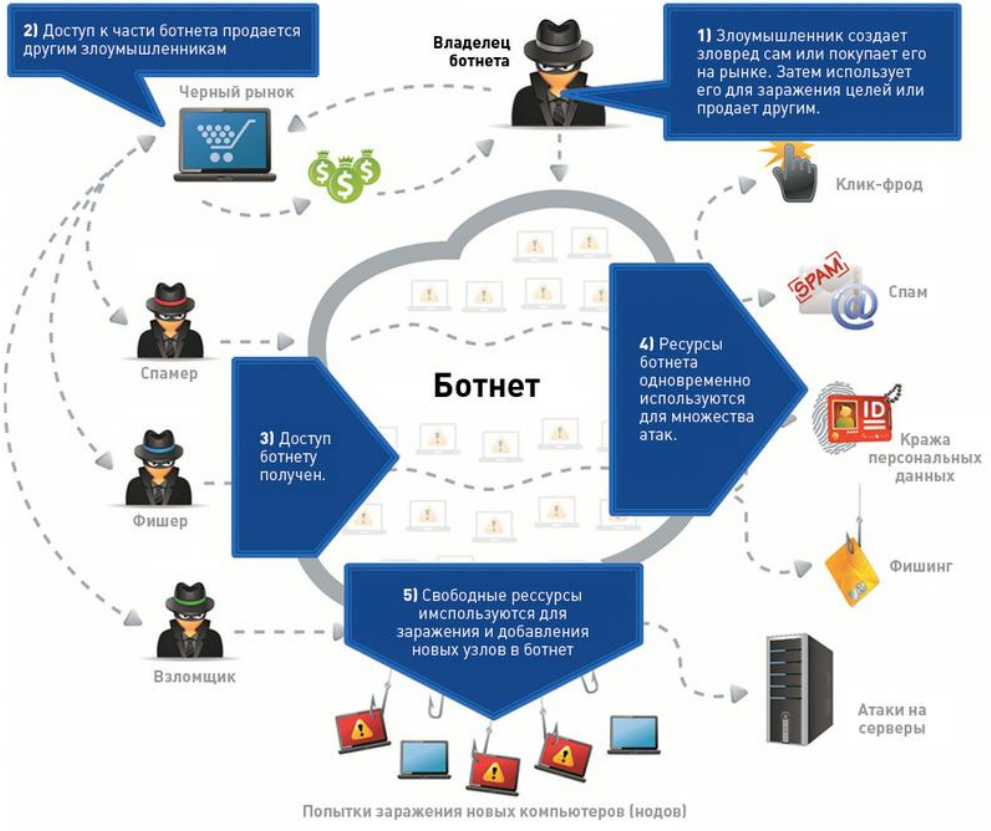
- Интерес

Построение ботнетов, не редко связанно с исследованиями.

Здесь могла бы быть
Ваша реклама.

google drive не позволяет заливать гифки(

Статистика собранная анонимным хакером.



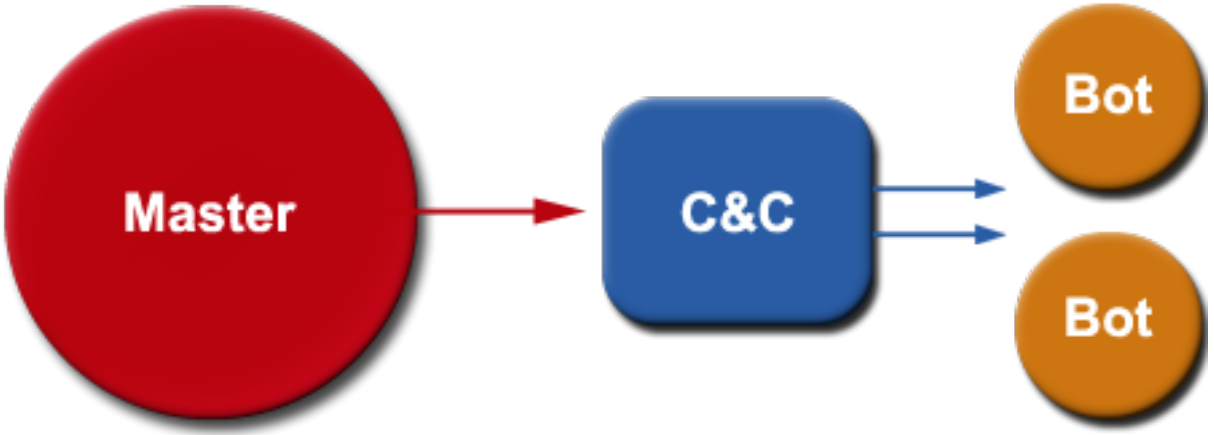
Способы реализации ботнетов.

Немного истории

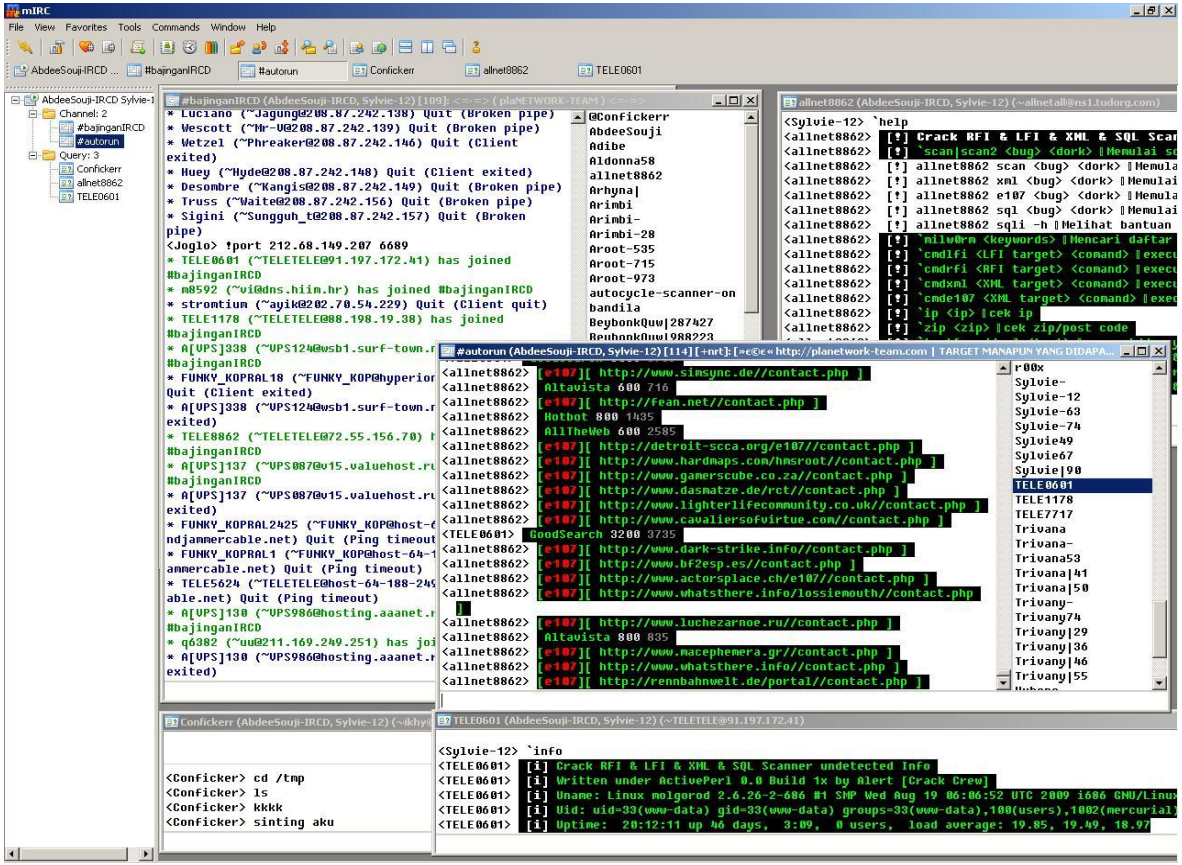
В 1993 году Jeff Fisher Robey Pointer написали EggDrop IRC-бот, который существует и по сей день.

Архитектура ботнета

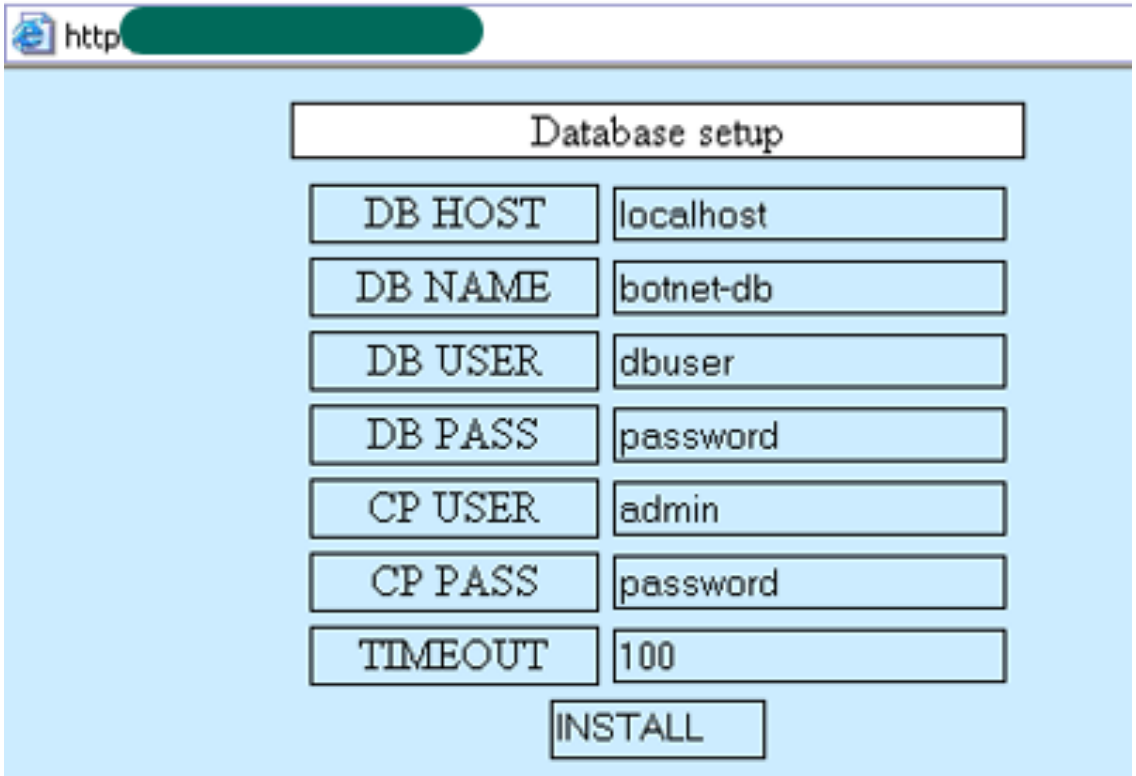
- Централизованная
  - HTTP/IRC
  - DNS server
  - TrustRing
- Децентрализованная
  - Peer-2-Peer
  - Случайная



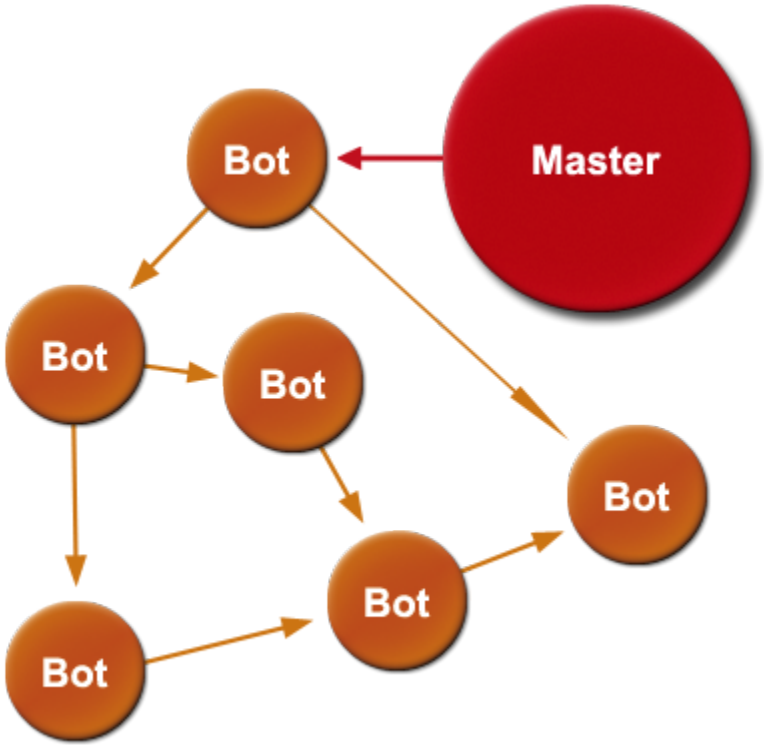
Централизованная архитектура



Централизованная архитектура



Централизованная архитектура



Децентрализованная архитектура

Основные команды

- Update
  - загрузить новую версию бота
- Flood
  - начать DoS атаку сервера
- Spam
  - загрузить шаблон спам сообщения
- Proxy
  - использовать машину как прокси-сервер

Command	Description
delete <filename>	Delete a specified file
execute <filename>	Execute a specified file
rename <origfile> <newfile>	Rename a specified file
makedir <dirname>	Create a specified directory
startkeylogger	Starts the on-line keylogger
stopkeylogger	Stops the keylogger
sendkeys <keys>	Simulates key presses
keyboardlights	Flashes remote keyboard lights 50x
passwords	Lists the RAS passwords in Windows 9x systems
listprocesses	Return a list of all running processes

Command	Description
listprocesses	Return a list of all running processes
killprocess <processname>	Kills the specified process
threads	Returns a list of all running threads
killthread < number >	Kills a specified thread
disconnect <number>	Disconnect the bot for number seconds
reboot	Reboot the system
cd-rom <0/1>	Open/close cd-rom
opencmd	Starts cmd.exe (hidden)
cmd <command>	Sends a command to cmd.exe
get <filename>	Triggers DCC send on bot
update <url>	Updates local copy of the bot code

Примеры команд SpyBot

Как командовать армией?

- IP-адрес хорошо скрытый в коде бота
  - Для получения команд бот использует IP хорошо “зашитый” в его коде
  - IP адрес можно заблокировать, сделав бота бесполезным

Как командовать армией?

- Через DNS сервер
  - Зашитый в коде бота адрес DNS сервера
  - Сложно отследить, особенно если ботмастер меняет сервера.
  - Проще продолжить атаку с чистого DNS
  - При сбое, создается новый адресс для переподключения.

Как командовать армией?

- Distributed(распределенный) DNS service
  - Сложнее всего обнаружить
  - Ботнет запускает собственный DNS
  - Используются большие номера портов, чтобы избежать обнаружения устройствами безопасности и шлюзами

Botnet Name	% of Spam	Spam per Day	Spam per Bot per Minute	Estimated Botnet Size	Geographical Distribution
Rustock	28.5%	13.82 billion	117	470,000 to 690,000	USA (11%), India (9%), Russia (6%)
Bagle	17.2%	8.31 billion	176	180,000 to 280,000	Russia (22%), India (8%), Columbia (7%)
Festi	8.7%	4.20 billion	77	210,000 to 320,000	India (12%), Vietnam (11%), Indonesia (10%)
Cutwail	4.5%	2.17 billion	33	250,000 to 380,000	Indonesia (12%), India (11%), Vietnam (8%)
Lethic	4.1%	1.98 billion	43	180,000 to 270,000	Russia (12%), India (9%), Ukraine (5%)
Grum	3.4%	1.64 billion	111	56,000 to 84,000	Brazil (15%), India (11%), Russia (8%)
Xarvester	2.8%	1.36 billion	125	43,000 to 65,000	Spain (16%), UK (11%), France (10%)
Maazben	2.5%	1.20 billion	15	300,000 to 450,000	Brazil (18%), Russia (15%), India (8%)
Donbot	0.3%	149.58 million	148	4,000 to 6,000	Columbia (11%), India (10%), Italy (10%)
Gheg	0.1%	43.33 million	19	9,000 to 13,000	Indonesia (20%), Argentina (16%), India (13%)
Other, smaller Botnets	1.5%	47.44 million	11	250,000 to 380,000	-
Un-classified Botnets	9.6%	4.67 billion	69	270,000 to 400,000	-
Total Botnet Spam	**83.1%**	**39.61** billion	**79**	**2.22 million to 3.34 million**	-

Количество спама рассылаемое ботами

Крупные ботнеты

- Zeus
  - DDoS,кража аккаунтов.
- Torpig
  - кража данных: кредитные карты, лицензионные ключи и т.д.
- Waledac
  - спам, DDoS.

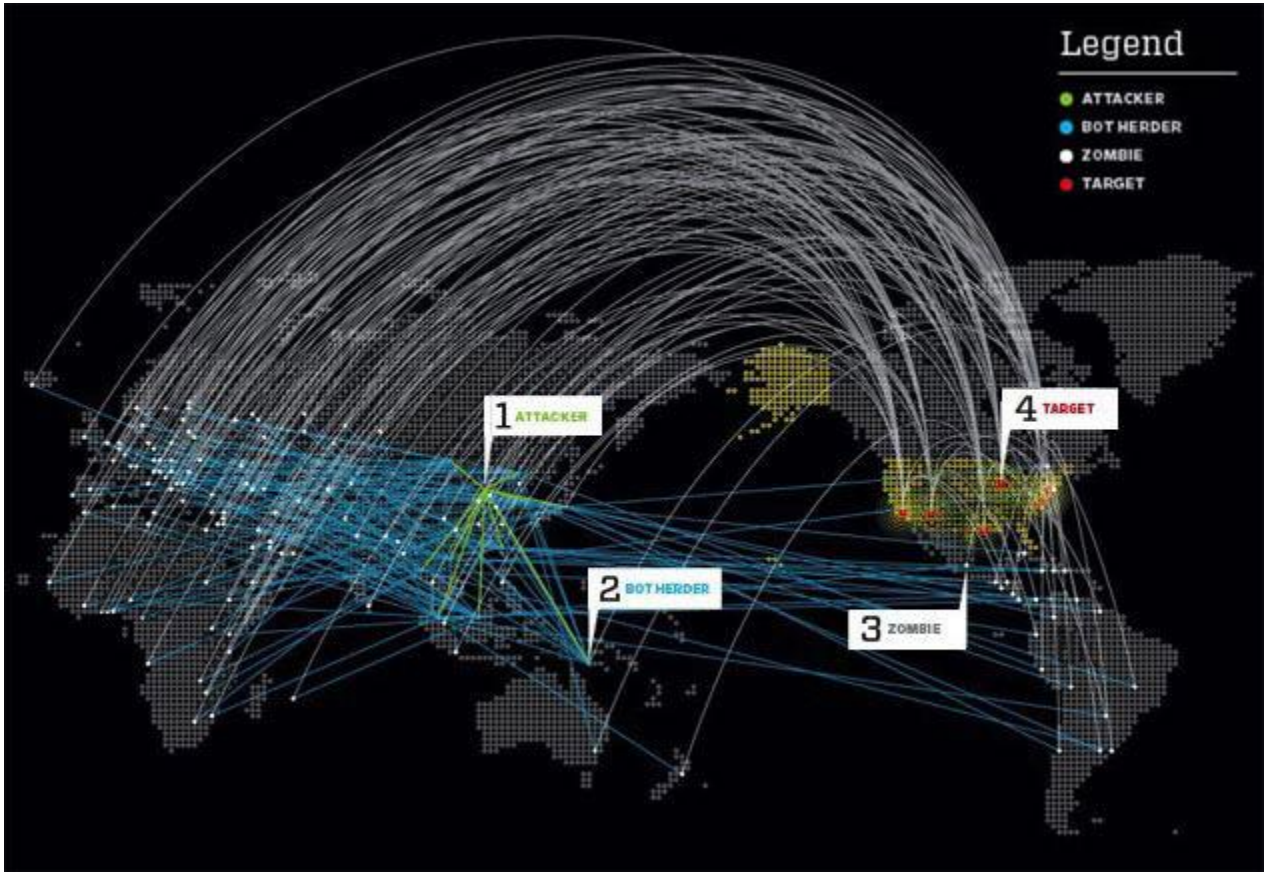


Иллюстрация процесса DDoS

```
suffix =  ["anj", "ebf", "arm", "pra", "aym", "unj",
    "ulj", "uag", "esp", "kot", "onv", "edc"]

def generate_daily_domain():
    t = GetLocalTime()
    p = 8
    return generate_domain(t, p)

def scramble_date(t, p):
    return (((t.month ^ t.day) + t.day) * p) +
        t.day + t.year

def generate_domain(t, p):
    if t.year < 2007:
        t.year = 2007
    s = scramble_date(t, p)
    c1 = (((t.year >> 2) & 0x3fc0) + s) % 25 + 'a'
    c2 = (t.month + s) % 10 + 'a'
    c3 = ((t.year & 0xff) + s) % 25 + 'a'
    if t.day * 2 < '0' ||  t.day * 2 > '9':
        c4 = (t.day * 2) % 25 + 'a'
    else:
        c4 = t.day % 10 + '1'
    return c1 + 'h' + c2 + c3 + 'x' + c4 +
        suffix[t.month - 1]
```

Генерация домена в Torpig

За 10 дней

- обнаруженно 180 тыс ПК и около 1.2 млн IP
- Полученно более 70Гб информации о аккаунтах пользователей.
- Полученно 8310 аккаунтов PayPal, Capital One, E*Trade и Chase
- Злоумышленники потеряли $8.3 млн

Результаты исследования Torpig

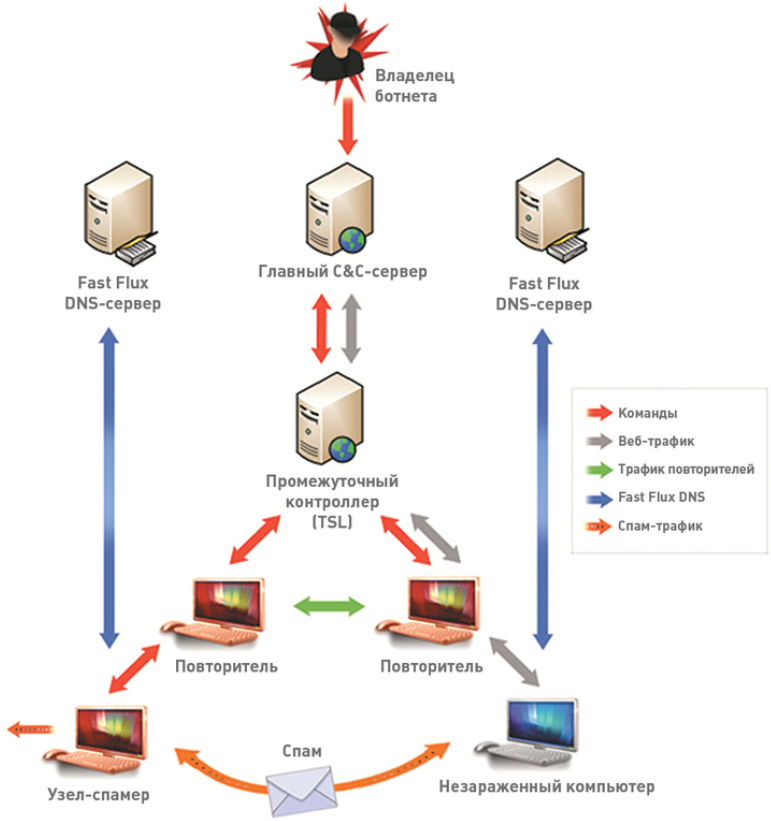
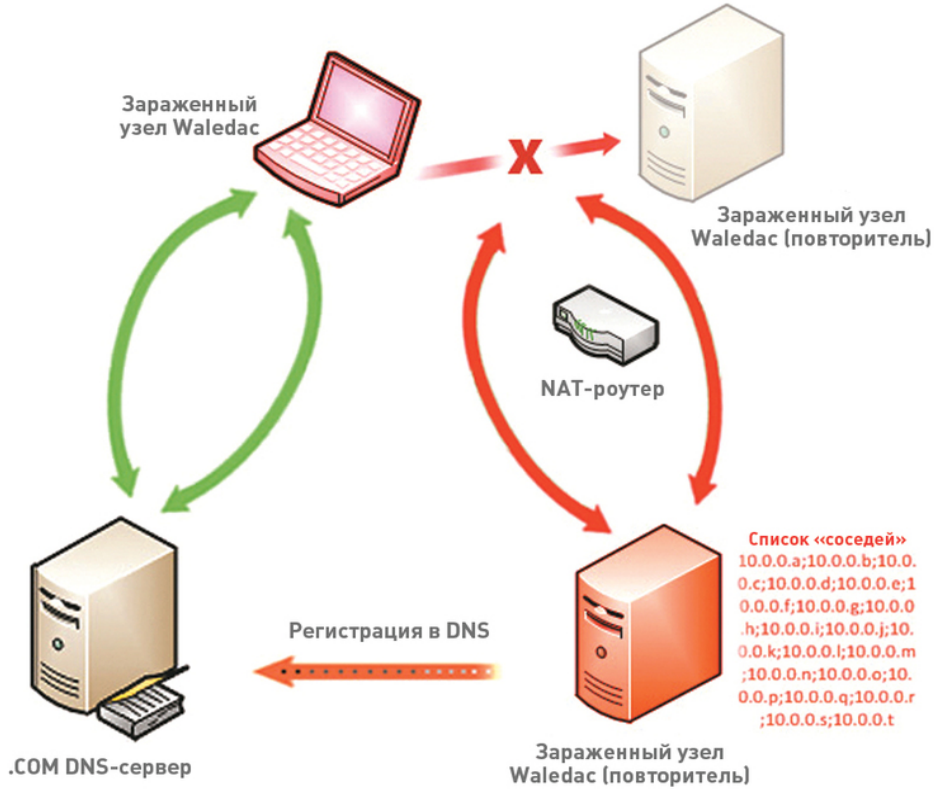
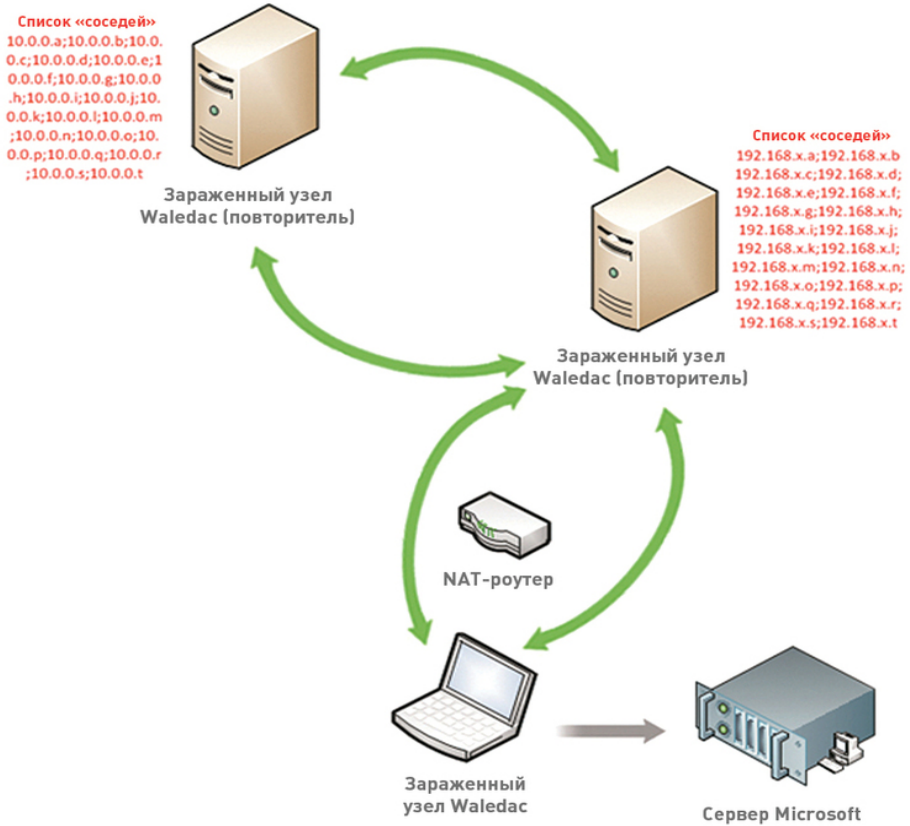


Схема работы Waledac

Способ распределения обязанностей



Подмена DNS сервера



Уборка троянов с машин