# Bot-Trek Secure Bank/Portal

## Система раннего обнаружения мошенничества на стороне пользователей

# Статистика Q2’2014-Q1’2015, Россия

Хищения в интернет-банкинге на сумму
2 649 422 000 рублей

**72%** Хищения в интернет-банкинге у юридических лиц

**24%** Целевые атаки на банки

**2%** Хищения у физических лиц с Android-троянами

**2%** Хищения в интернет-банкинге у физических лиц

# Мошеннические группы Q2’2014-Q1’2015

| Группы, работающие по компаниям | Группы, работающие по физическим лицам через интернет-банкинг | Группы, работающие по физическим лицам через мобильный клиент-банк |
|---|---|---|
| Cork | Proxy | ~~Reich~~ |
| Lurk | ~~PhishEye~~ | Greff |
| ~~Shiz~~ | ~~Infinity~~ | March |
| ~~Ranbyus~~ | | ~~Waplook~~ |
| ~~Infinity~~ | | Ada |
| Toplel[New] | | Ada2[New] |
| Kontur (Buhtrap)[New] | | Cron[New] |
| Uni_chthonic[New] | | ApiMaps[New] |
| Prosecutor[New] | | Tark[New] |
| Kronos_Nalog[New] | | Xruss[New] |
| Yebot[New] | | MobiApps[New] |
| | | Sizeprofit[New] |
| | | Mikorta[New] |
| | | Webmobil[New] |
| | | Group 404[New] |

# Векторы атак

| Название группы | Используемые вредоносные программы | Способ распространения | Способ хищения |
|---|---|---|---|
| Lurk | Lurk | Набор эксплоитов Angler Exploit Kit | Автозалив<br>Автоподмена |
| Cork | Corkow, RMS, HVNC, AmmyAdmin | Набор эксплоитов CottonCastle/Niterix | |
| ToplelNew | Pony, RDPdoor | Электронная почта | Удаленный доступ |
| Kontur (Buhtrap)New | NSIS.Downloader, LiteManager | | |
| Uni_chthonicNew | Chthonic (модификация ZeusVM) | | |
| ProsecutorNew | ChePro | | |
| Kronos_NalogNew | Kronos и система автоподмены | | |
| YebotNew | Yebot | | |
| Proxy | Proxy.adder | Набор эксплоитов GrandSoft | Социальная инженерия<br>Перевыпуск SIM |

# Lurk: автоматическая подмена счета

Используется для совершения хищений с банковских счетов через IBANK2 методом автоматической подмены реквизитов получателя («автозалив»).

Имеет встроенный модуль Mimikatz, позволяющий извлекать учетные данные Windows из LSA.

2011 2014 2015 2016

Позже были добавлены «толстые клиенты» систем ДБО: СБРФ, BSS, ВТБ, Промсвязьбанк. Добавлен модуль HVNC для удаленного управления компьютером жертвы.

«Автозалив» под «тонкого» клиента. В конфигурационном файле более 50 банков.

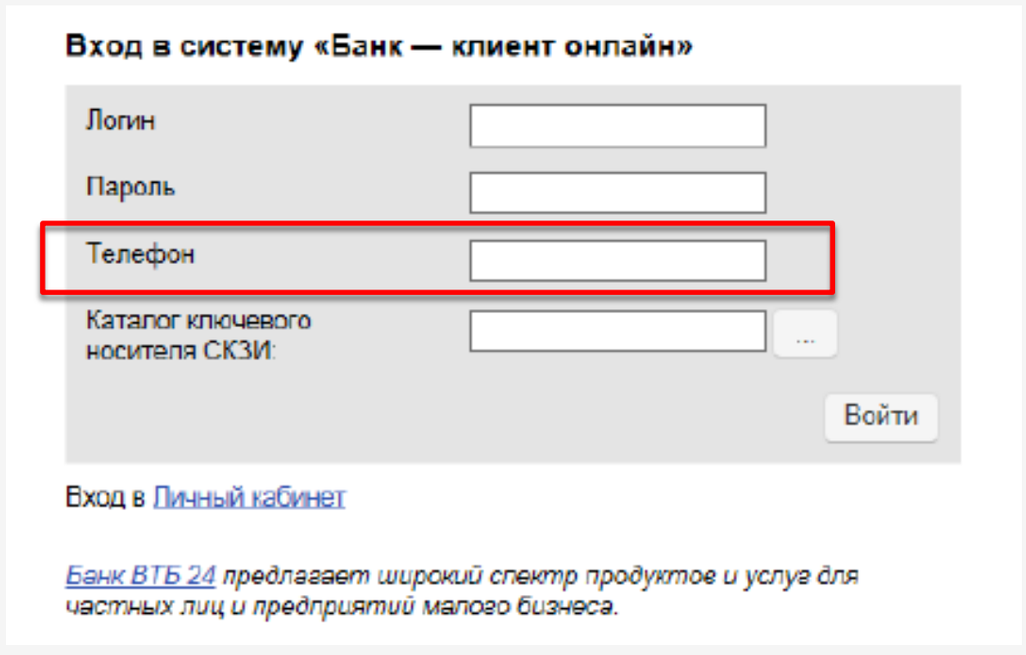
# Lurk: hackers’ swisstool

| Имя команды | Соответствующий функционал программы |
|---|---|
| get_file | Отправить на управляющий сервер файл с определенным именем. |
| get_process_list | Отправить на управляющий сервер информацию о запущенных процессах. |
| get_java_cache | Отправить на управляющий сервер содержимое каталога с именем «%APPDATA%\Sun\Java\Deployment\cache» или каталога, указанного в поле с именем «deployment.user.cachedir» файла конфигурации «%APPDATA%\Sun\Java\Deployment\deployment.properties» |
| get_software | Отправить на удаленный сервер информацию об установленном ПО. |
| dir_list | Отправить на удаленный сервер информацию о подкаталогах указанного каталога. |
| exec | Загрузить с удаленного сервера файл и выполнить его. |
| get_storage | Отправить на управляющий сервер данные из хранилища исследуемой программы. |
| set_storage | Переназначить хранилище исследуемой программы |
| del_storage | Удалить хранилище исследуемой программы. |
| init_rdp | Предоставить удаленный доступ к ЭВМ по протоколу RDP |
| set_video_capture | Начать процедуру снятия видео происходящего на экране. |
| back_connect | В зависимости от параметров команды осуществляется либо настройка «Proxy» сервера на ЭВМ или VNC сервера. Прослушивание IP адреса 127.0.0.1 позволяет инициализировать соединение по VNC даже если ЭВМ имеет выход в сеть Интернет с использованием NAT (Network Address Translation). |
| body_update | Загрузка и запуск файла с последующей остановкой программы и ее удалением. |
| plugin_update | Загрузка дополнительного подключаемого модуля |
| plugin_uninstall | Удаление подключаемого модуля |

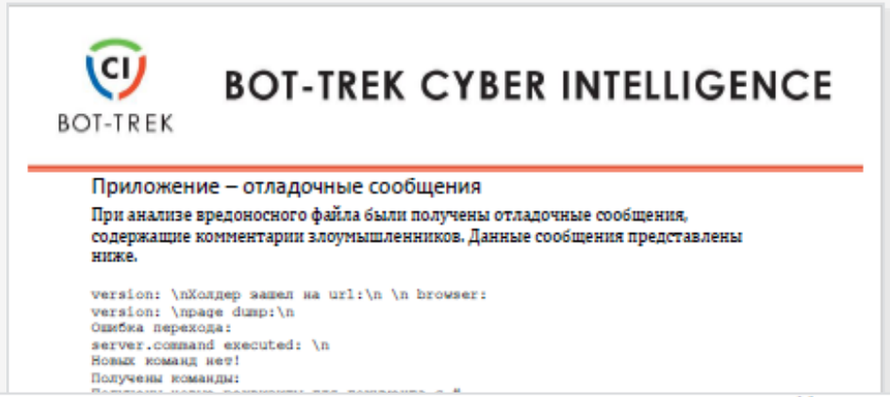
# Lurk: веб-инъекция (170-250Кб)

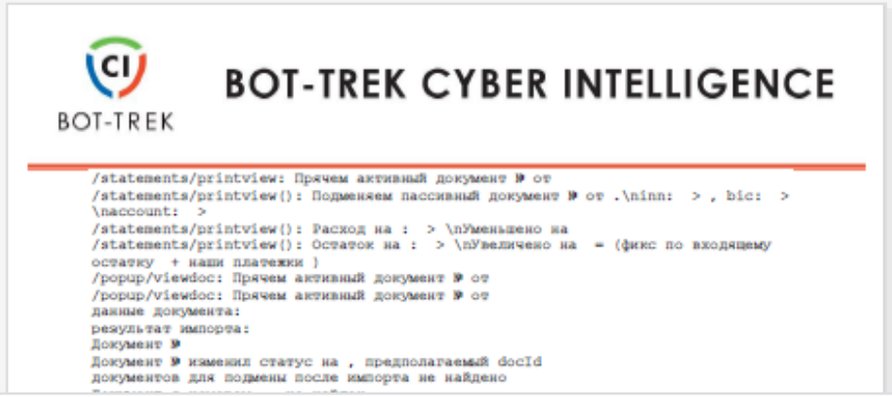
```
<script rel = "F0V48wVkyyY"> (function(x, z) {
    var g, a = {
        debug: 0,
        version: "2.91",
        SID: "F0V48wVkyyY",
        cache: {},
        e: function(a) {
            return (a && (a.message || a.description || a.msg) || a) + ""
        },
        isLocal: function(a) {
            try {
                return !/^http/i.test(a || location.href) || !location.hostname || /^(127|19
            } catch (d) {
                return !1
            }
        },
        ver: function() {
            return a.version + " (" + a.revision + ")" + (a.app ? " " + a.app.version : "") 
        }
    };
    a.e.stack = [];
    var M = a.URL = {
        ADMIN_SEND: "/eNCgq6ngmR6",
        ADMIN_RECV: "/OfO7jEcWn0Yu",
        ADMIN_STAT: "/N0uVGcsXy6",
        BOT_TEMPORARY: "/g2yGJj9wBSPi",
        BOT_PERMANENT: "/0XQDwE9hFnuF6",
        BOT_REPLACE: "/E1Z9bMLE7dP",
        BOT_UPLOAD: "/Cp9e0UOUn"
    };
```

# Lurk: подмена форм

# Lurk: подмена реквизитов




```
/statements: подмена ()\nвходящий остаток: >
/statements: подмена ()\nсумарный расход: >
/statements: подмена ()\nисходящий остаток: >
/statements/online: Скрываем активный документ № от
/statements/online: Подменяем пассивный документ № от .\nbic: > \naccount: >
/statements/online: подмена ()\nвходящий остаток: >
/statements/online: подмена ()\nисходящий остаток: >
/statements/printview(): Входящий остаток на : > \nУвеличено на
```

# Lurk: лог работы на «жертве»

```
[{\"bank\":\"b        .ru\",\"message\":\"DEBUG: Холдер        вошел
под именем                                  \

{\"bank\":\"b        .ru\",\"message\":\"DEBUG: Холдер авторизовался используя
данные        Qwerty321. Mespro pass: Qwerty4321

{\"bank\":\"b        .ru\",\"message\":\"INFO: Найден счет . баланс:

q.type=\"COMMAND\",q.status=\"RTE\",m=n.doc.find(q));
if(m&&!a.restrictPayments)l.debug([\"Для документа №s использован дроп #s. amount: s\",
c,m.id,g],null,m.id);else return currentStage=l.stage,
l.debug([\"Для документа №s не катит ни один дроп.\"])
```

# Bot-Trek Secure Bank – система раннего предупреждения мошеннических операций в системах онлайн-платежей

Не требует установки на устройства клиента

Мгновенно распространяется на всю клиентскую базу

Отслеживает новые типы атак и схемы мошенничества

Интегрируется с антифрод системами через API

# Bot-Trek Secure Bank выявляет

Банковские трояны

Внедрение зловредных инъекций

Подмена реквизитов получателя («автозалив»)

Несанкционированное удаленное подключение

Фишинг- и фарминг-атаки

Проникновение через 0-day уязвимости

# Lurk: конфигурационный файл


```
KLRules:1{"id":2,"process":"*","window":"*","caption":"вход","control":"*"}
KLRules:20{"id":120,"process":"KeePass.exe","window":"*","caption":"*","control":"*"}
KLRules:21{"id":121,"process":"*","window":"*","caption":"logon","control":"*"}
KLRules:22{"id":122,"process":"*","window":"*","caption":"wealth-lab","control":"*"}
KLRules:23{"id":123,"process":"*","window":"*","caption":"Quik","control":"*"}
KLRules:25{"id":124,"process":"*","window":"*","caption":"Trader","control":"*"}
KLRules:26{"id":125,"process":"*","window":"*","caption":"SmartX","control":"*"}
KLRules:49{"id":146,"process":"*","window":"*","caption":"Apple ID","control":"*"}
KLRules:53{"id":150,"process":"*","window":"*","caption":"Hetzner Online GmbH - Robot","control":"*"}
KLRules:56{"id":153,"process":"*","window":"*","caption":"Gmail","control":"*"}
KLRules:58{"id":154,"process":"*","window":"*","caption":"retail","control":"*"}
KLRules:59{"id":155,"process":"*","window":"*","caption":"kitty","control":"*"}
KLRules:60{"id":157,"process":"*","window":"*","caption":"RemoteApp","control":"*"}
KLRules:61{"id":158,"process":"qiwicashier.exe","window":"*","caption":"*","control":"*"}
KLRules:62{"id":159,"process":"*","window":"*","caption":"qiwi","control":"*"}
KLRules:74{"id":170,"process":"*","window":"*","caption":"УГМК","control":"*"}
KLRules:77{"id":173,"process":"*","window":"*","caption":"Log In","control":"*"}
KLRules:78{"id":174,"process":"*","window":"*","caption":"Антиквар","control":"*"}
KLRules:239{"id":321,"process":"*","window":"*","caption":"BS-Client","control":"*"}
KLRules:240{"id":322,"process":"*","window":"*","caption":"Альфа-Клиент","control":"*"}
KLRules:243{"id":325,"process":"*","window":"*","caption":"ELBA","control":"*"}
KLRules:248{"id":329,"process":"*","window":"*","caption":"АЦК-БФТ","control":"*"}
KLRules:249{"id":330,"process":"*","window":"*","caption":"Банк Клиент Онлайн","control":"*"}
KLRules:252{"id":333,"process":"*","window":"*","caption":"РОССИЙСКИЙ КАПИТАЛ","control":"*"}
KLRules:254{"id":335,"process":"*","window":"*","caption":"КриптоПро CSP","control":"*"}
KLRules:307{"id":383,"process":"*","window":"*","caption":"Межведомственные запросы","control":"*"}
KLRules:312{"id":40,"process":"*","window":"*","caption":"СУФД","control":"*"}
KLRules:381{"id":78,"process":"*","window":"*","caption":"Bot-Trek","control":"*"}
```

# Результаты…

Существуют целые «магазины», которые постоянно пополняются новыми аккаунтами с бонусами

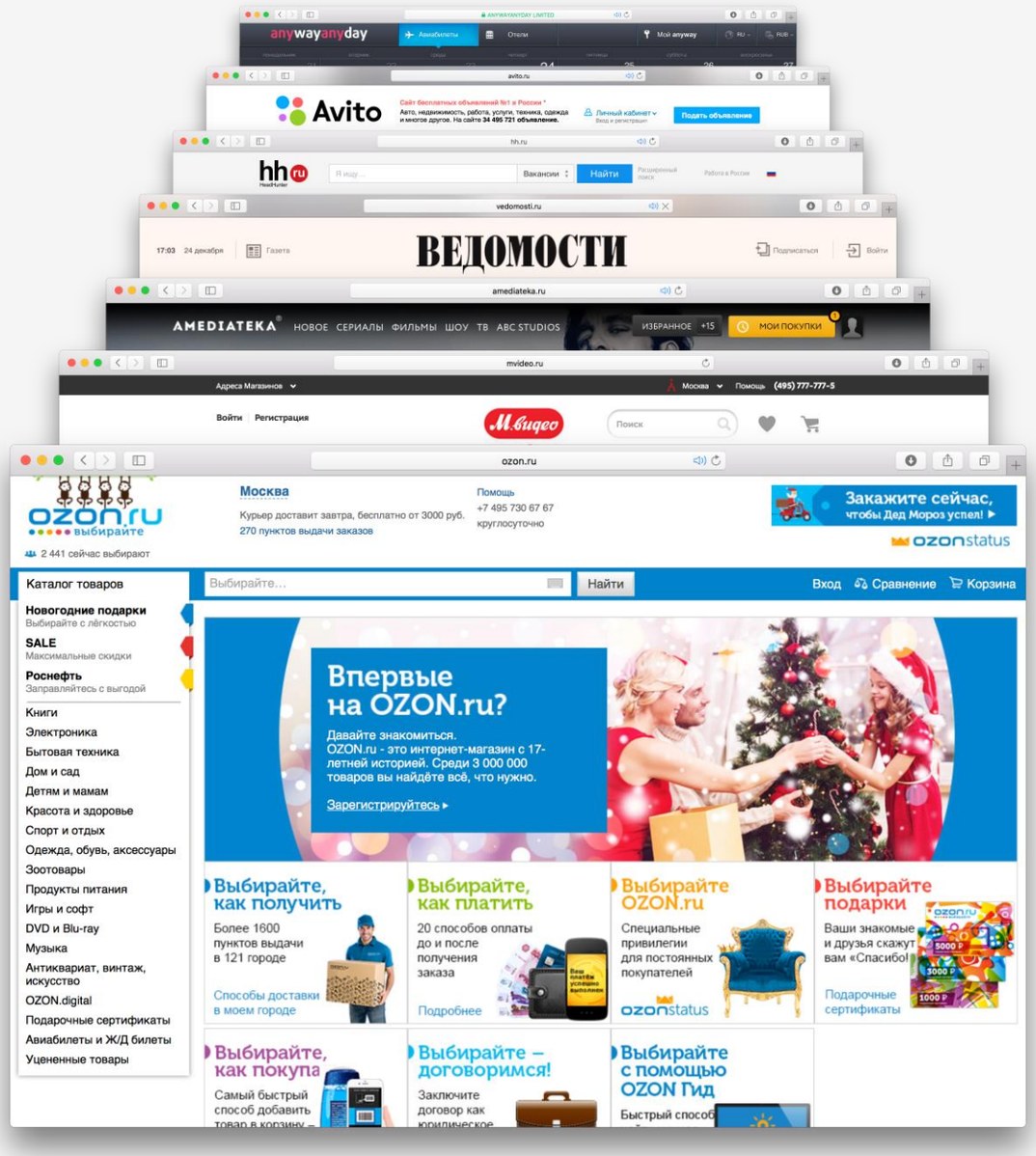
# Виды мошенничества на порталах

Несанкционированный доступ в личные кабинеты

Кража карточных данных

«Обнал» бонусных карт/миль

Оплата ворованными платежными картами




Мошеннические объявления

Совместное использование платной подписки

Использование «ботов»

Реклама конкурентов на страницах портала

# Bot-Trek Secure Portal – система раннего обнаружения мошенничества на стороне пользователей – самого слабого звена в обеспечении безопасности интернет-бизнеса

Не требует установки на устройства клиента

Не требует установки в IT-инфраструктуру и дополнительных инвестиций

API для автоматизации реагирования на мошенничество в режиме реального времени

Дает дополнительную информацию о пользователе

# Bot-Trek Secure Portal выявляет

Доступ в личные кабинеты третьими лицами

Мошенничество с платежными картами (сторонняя p2p-страница)

Использование ворованных картам, эл. кошельков, бонусов

Фишинговые сайты и применение социальной инженерии

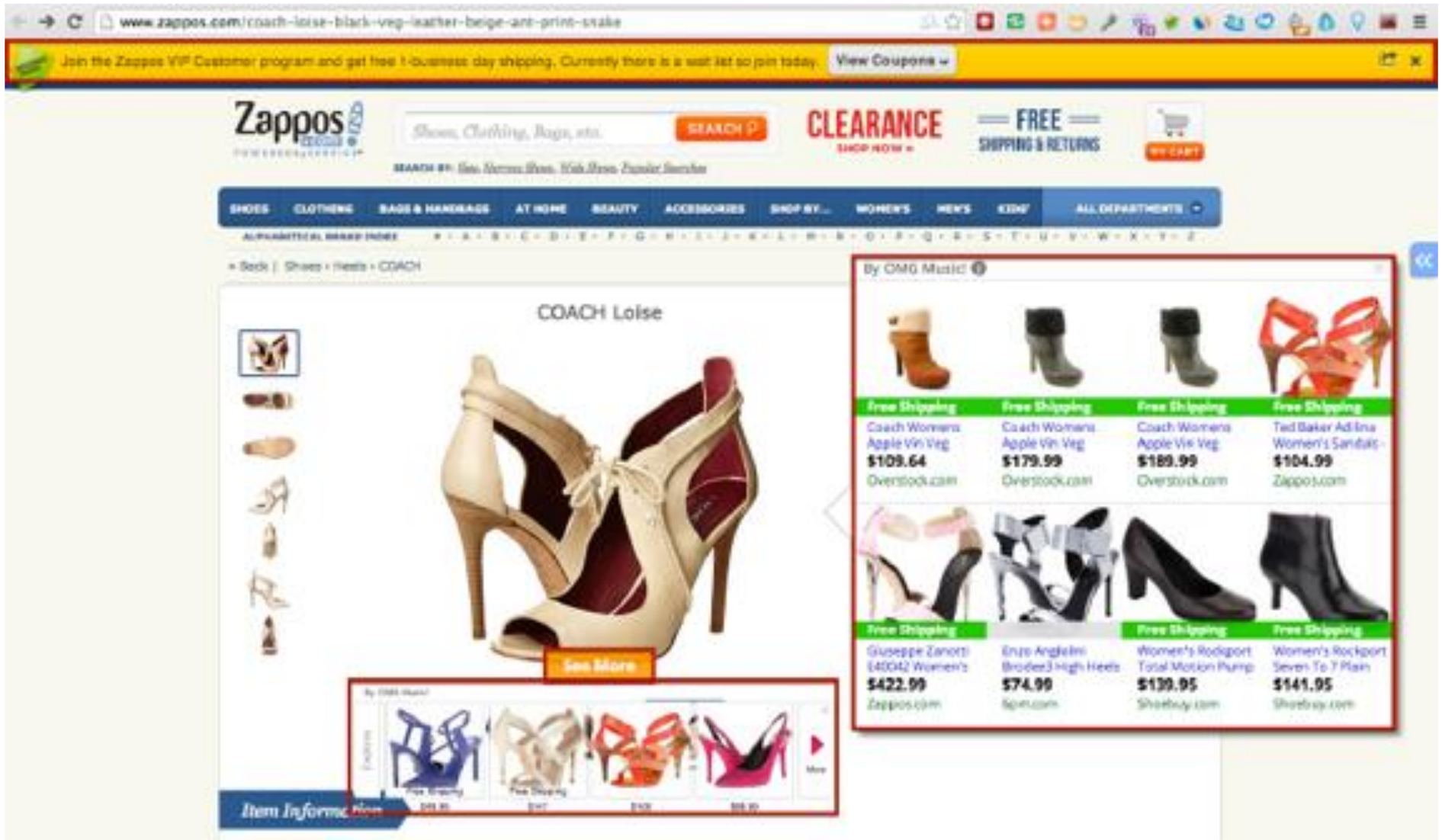
Стороннюю рекламу при посещении официального сайта

Действия на портале от третьих лиц

Использование «ботов» для мошенических действий на сайте

Новые виды мошенничества на стороне пользователя

# Bot-Trek Secure Portal предотвращает




* на примере сайта Zappos

# ВЫ НЕ МОЖЕТЕ КУПИТЬ АБСОЛЮТНУЮ ЗАЩИТУ ОТ КИБЕРУГРОЗ

# НО ВЫ МОЖЕТЕ КУПИТЬ ВРЕМЯ НА ИХ ПРЕДОТВРАЩЕНИЕ

# Спасибо!

Павел Крылов

krylov@group-ib.ru

+7 968 014-88-62