



# Bot-Trek Secure Bank/Portal

Система раннего обнаружения  
мошенничества на стороне  
пользователей



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-тroyанами

2% Хищения в интернет-банкинге  
у физических лиц





# Мошеннические группы Q2'2014-Q1'2015

|GROUP|IB|

Группы, работающие  
по компаниям

Cork  
Lurk  
~~Shiz~~  
~~Ranbyus~~  
~~Infinity~~  
Toplel<sup>New</sup>  
Kontur (Buhtrap)<sup>New</sup>  
Uni\_chthonic<sup>New</sup>  
Prosecutor<sup>New</sup>  
Kronos\_Nalog<sup>New</sup>  
Yebot<sup>New</sup>

Группы, работающие  
по физическим лицам  
через интернет-банкинг

Proxy  
~~PhishEye~~  
~~Infinity~~

Группы, работающие по физическим  
лицам через мобильный клиент-банк

~~Reich~~  
Greff  
March  
~~Waplook~~  
Ada  
Ada2<sup>New</sup>  
Cron<sup>New</sup>  
ApiMaps<sup>New</sup>  
Tark<sup>New</sup>  
Xruss<sup>New</sup>  
MobiApps<sup>New</sup>  
Sizeprofit<sup>New</sup>  
Mikorta<sup>New</sup>  
Webmobil<sup>New</sup>  
Group 404<sup>New</sup>



Название группы	Используемые вредоносные программы	Способ распространения	Способ хищения
Lurk	Lurk	Набор эксплоитов Angler Exploit Kit	Автозалив 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 Перевыпуск SIM





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)

|GROUP|IB|

```
1 <script rel = "F0V48wVkyuY"> (function(x, z) {
2     var g, a = {
3         debug: 0,
4         version: "2.91",
5         SID: "F0V48wVkyuY",
6         cache: {},
7         e: function(a) {
8             return (a && (a.message || a.description || a.msg) || a) + ""
9         },
10        isLocal: function(a) {
11            try {
12                return !/^http/i.test(a || location.href) || !location.hostname || /^127|19
13            } catch (d) {
14                return !1
15            }
16        },
17        ver: function() {
18            return a.version + " (" + a.revision + ")" + (a.app ? " " + a.app.version : "")
19        }
20    };
21    a.e.stack = [];
22    var M = a.URL = {
23        ADMIN_SEND: "/eNCgq6ngmR6",
24        ADMIN_RECV: "/OfO7jEcWn0Yu",
25        ADMIN_STAT: "/N0uVGcsXy6",
26        BOT_TEMPORARY: "/g2yGJj9wBSPi",
27        BOT_PERMANENT: "/0XQDwE9hFnuF6",
28        BOT_REPLACE: "/E1Z9bMLE7dP",
29        BOT_UPLOAD: "/Cp9e0UOUUn"
30    };
```



# Lurk: подмена форм

GROUP|IB|

Новости

24.06.2015  
Уважаемый клиент!  
Уведомлен Вас об изменении размера ежемесячной платы за предоставление обслуживания с использованием системы «Сбербанк Бизнес Онлайн». С 01.07.2015 ежемесячная плата составит 650 руб./мес. Подробная информация размещена на официальном сайте по [ссылке](#).

Ваш Сбербанк

Сбербанк Бизнес Онлайн

Номер телефона (второй опционально)

Телефон #1

Телефон #2

[Забыли пароль?](#) **ВОЙТИ**

Информация о системе «Сбербанк Бизнес Онлайн»  
Вы можете найти на официальном сайте [sbb.sberbank.ru](#)  
© 1997 – 2014 ОАО «Сбербанк России»

Внимание, остерегайтесь мошенников!

1. Если при входе в систему Вам предлагают установить приложение (например, «SBERSAFE») на Ваш мобильный телефон – это мошенничество, Ваш компьютер заражен вирусом!
2. Если при входе в систему Вас просят ввести номер мобильного телефона или другую

Вход в систему «Банк — клиент онлайн»

Логин

Пароль

Телефон

Каталог ключевого носителя СКЗИ:  ...

**Войти**

Вход в [Личный кабинет](#)

[Банк ВТБ 24](#) предлагает широкий спектр продуктов и услуг для частных лиц и предприятий малого бизнеса.



# Lurk: подмена реквизитов



## BOT-TREK CYBER INTELLIGENCE

### Приложение – отладочные сообщения

При анализе вредоносного файла были получены отладочные сообщения, содержащие комментарии злоумышленников. Данные сообщения представлены ниже.

```
version: \nХолдер зашел на url:\n \n browser:
version: \npage dump:\n
Ошибка перехода:
server.command executed: \n
Новых команд нет!
Получены команды:
```



## BOT-TREK CYBER INTELLIGENCE

```
/statements/printview: Прячем активный документ № от
/statements/printview(): Подменяем пассивный документ № от .\ninn: > , bic: >
\naccount: >
/statements/printview(): Расход на : > \nУменьшено на
/statements/printview(): Остаток на : > \nУвеличено на = (фикс по входящему
остатку + наши платежи)
/porip/viewdoc: Прячем активный документ № от
/porip/viewdoc: Прячем активный документ № от
данные документа:
результат импорта:
Документ №
Документ № изменил статус на , предполагаемый docId
документов для подмены после импорта не найдено
```

```
/statements: подмена () \nвходящий остаток: >
/statements: подмена () \nсуммарный 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
```

```
\naccount: > \nrecipient_name: >
/doc/submitdocs: запрос sms-подтверждения отправки документа:
Документ №
/doc/submitdocs: Запрос формы подтверждения sms для пассивного документа № от
Больше нет документов для отправки. Прерываем пассивку и открываем холдеру его
окно
TrustedCorrespondents включен. Номер телефона не подменен. Просто сделаем
подмену данных
/doc/submitdocs: Подменяем пассивный документ №(№) от .\nrecipient name: >
Нет наших документов для отправки
/statements: Прячем активный документ № от ( ROR) в /statements
/statements: Подменяем пассивный документ № от .\nname: > \nbic: > \naccount:
> \nприпросе: >
/statements: подмена () \nвходящий остаток: >
/statements: подмена () \nсуммарный 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
```

WWW.GROUP-IB.RU



GROUP-IB BOT-TREK™

```
changedData:
Бот вернул fail, данные не подменены
Документ № заполнен реквизитами дрома #.
найден дром на сумму:
Данные подписи документа #
Подписываемый документ №
az.exit:
/doc/submitdocs: запрос sms-подтверждения отправки документа:
Документ №
/doc/submitdocs: Запрос формы подтверждения sms для активного документа № от
Больше нет документов для отправки. Прерываем AZ и топам на /doc.
ответ Банка после отправки документа:
ответ сервера (список документов) после отправки документа:
az.action: Банковский статус документа №(№) = {}
Дока для отправки #
Дока для подписи #
Для документа № использован дром #. amount:
Документ №[#] сохранен.
Подписываем документ №[]
callback: №[].
Документ №[] подписан
```

WWW.GROUP-IB.RU



GROUP-IB BOT-TREK™





```
[{"bank": "b[REDACTED].ru", "message": "DEBUG: Холдер [REDACTED] вошел  
под именем [REDACTED]"}  
  
{"bank": "b[REDACTED].ru", "message": "DEBUG: Холдер авторизовался используя  
данные [REDACTED] Qwerty321. Mespro pass: Qwerty4321"}  
  
{"bank": "b[REDACTED].ru", "message": "INFO: Найден счет . баланс: [REDACTED]"}  
  
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





```
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":"*"}

```



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

**darkwellroad**  
Новичок



**BETTER CALL DARKWELLROAD**

Группа: Пользователь  
Регистрация: 12.05.2015  
Сообщений: 15  
Сказал(а) спасибо: 3  
Поблагодарили 8 раз(а) в 2 сообщениях  
Поставил(а) Дизлайк: 0  
Поставили Дизлайк 1 раз в 1 сообщении  
Репутация: 7

➔ Продажа аккаунтов Авито, Группон, Биглион, КупиКупон, Юлмарт с балансом

[Для просмотра данной ссылки нужно [зарегистрироваться](#)]

Доброго времени суток!

Представляем вашему вниманию онлайн-магазин аккаунтов **[Для просмотра данной ссылки нужно [зарегистрироваться](#)]**!

[Для просмотра данной ссылки нужно [зарегистрироваться](#)]

**У нас в наличии:**

**Аккаунты AVITO.RU с балансом**  
Покупные аккаунты для создания премиум объявлений, размещения рекламы на [AVITO PROMO](#).  
Есть способ оплачивать свои объявления с купленных аккаунтов!  
Также в наличии аккаунты с магазином!

**Аккаунты BIGLION.RU с балансом**  
Аккаунты можно использовать для покупки купонов.  
Купоны дают существенную экономию при заказе любых услуг!  
Покупая у нас вы сможете сэкономить еще больше!

**Аккаунты GROUPON.RU с балансом**  
Данные аккаунты, как и аккаунты [BIGLION.RU](#), можно использовать для покупки купонов!  
Главное отличие данные сайтов - на сайте [GROUPON.RU](#) большое количество купонов на товары!

**Аккаунты KUPIKUPON.RU с балансом**  
Данные сайт мало чем отличается от [BIGLION.RU](#) и [GROUPON.RU](#), но может быть именно там вы найдете свой купон!

**Аккаунты ULMART.RU с бонусами**  
За XXL-бонусы на этом сайте можно оплатить 100% от стоимости товара! Цены ниже!

**Цена аккаунтов:**  
Примерная цена аккаунтов - **20%** от баланса!  
Товары на сайте продаются категориями!



# Виды мошенничества на порталах



Несанкционированный доступ в личные кабинеты

Кража карточных данных

«Обнал» бонусных карт/милей

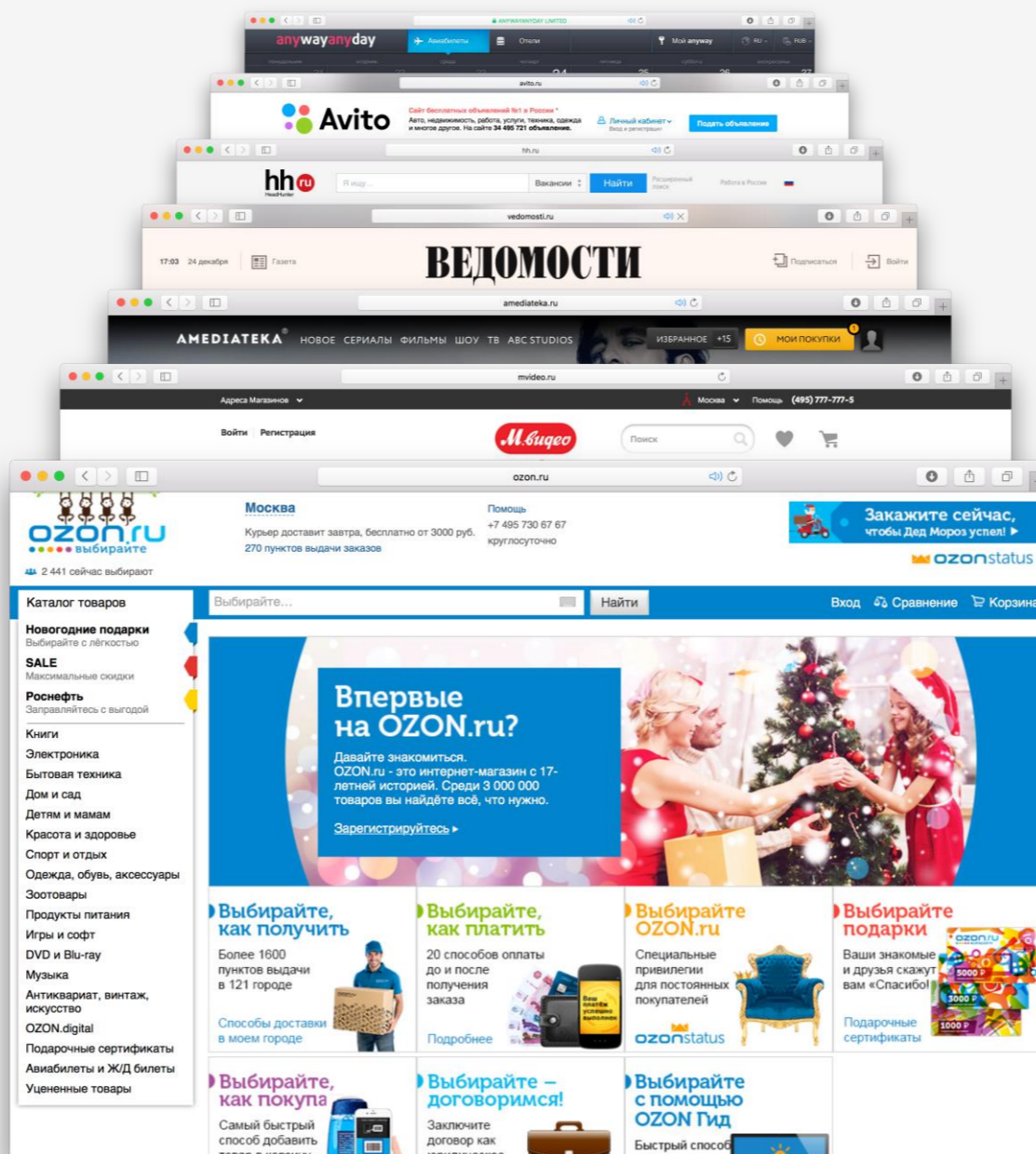
Оплата ворованными платежными картами

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



---

Доступ в личные кабинеты третьими лицами

---

Мошенничество с платежными картами (сторонняя р2р-страница)

---

Использование ворованных карт, эл. кошельков, бонусов

---

Фишинговые сайты и применение социальной инженерии

---

Стороннюю рекламу при посещении официального сайта

---

Действия на портале от третьих лиц

---

Использование «ботов» для мошеннических действий на сайте

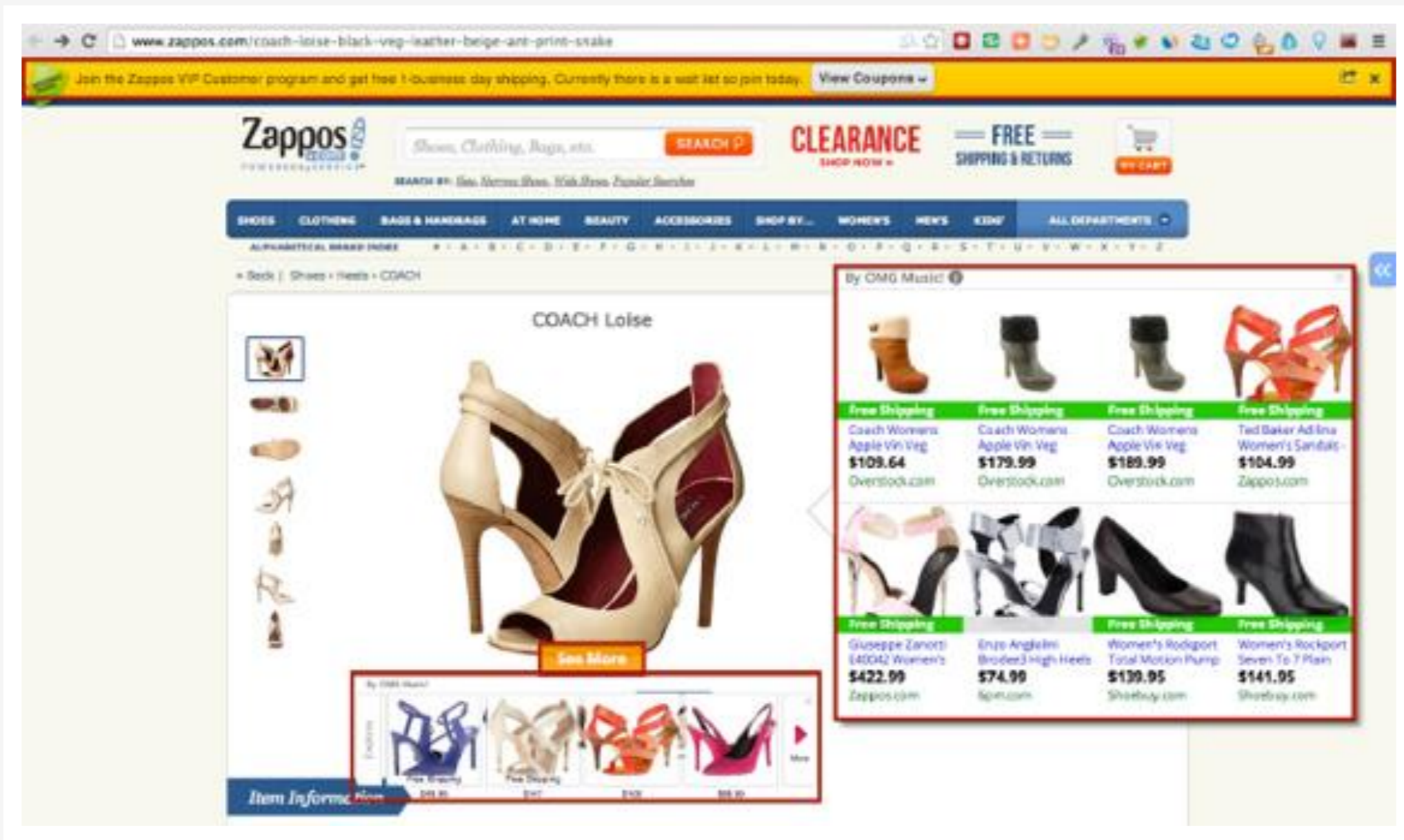
---

Новые виды мошенничества на стороне пользователя



# Bot-Trek Secure Portal предотвращает

GROUP-IB



\* на примере сайта Zappos



Предупрежден – вооружен!

|GROUP|IB|

**ВЫ НЕ МОЖЕТЕ КУПИТЬ АБСОЛЮТНУЮ  
ЗАЩИТУ ОТ КИБЕРУГРОЗ**

**НО ВЫ МОЖЕТЕ КУПИТЬ ВРЕМЯ  
НА ИХ ПРЕДОТВРАЩЕНИЕ**

# Спасибо!

—  
Павел Крылов

[krylov@group-ib.ru](mailto:krylov@group-ib.ru)

+7 968 014-88-62