Как не дать мошенникам заработать на вас и вашей компании в интернете

Дмитрий Русаков
Директор по развитию направления Brand Protection

О компании

Group-IB — одна из ведущих международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий

1000+

успешных расследований по всему миру, 150 особо сложных уголовных дел

$300 млн

возвращено клиентам Group-IB благодаря нашей работе

Официальный партнер Europol, полицейской службы Евросоюза

Рекомендована Организацией по безопасности и сотрудничеству в Европе (ОБСЕ)

Постоянный член Всемирного экономического форума

Threat Intelligence от Group-IB – в числе лучших мировых систем по оценке Forrester и Gartner

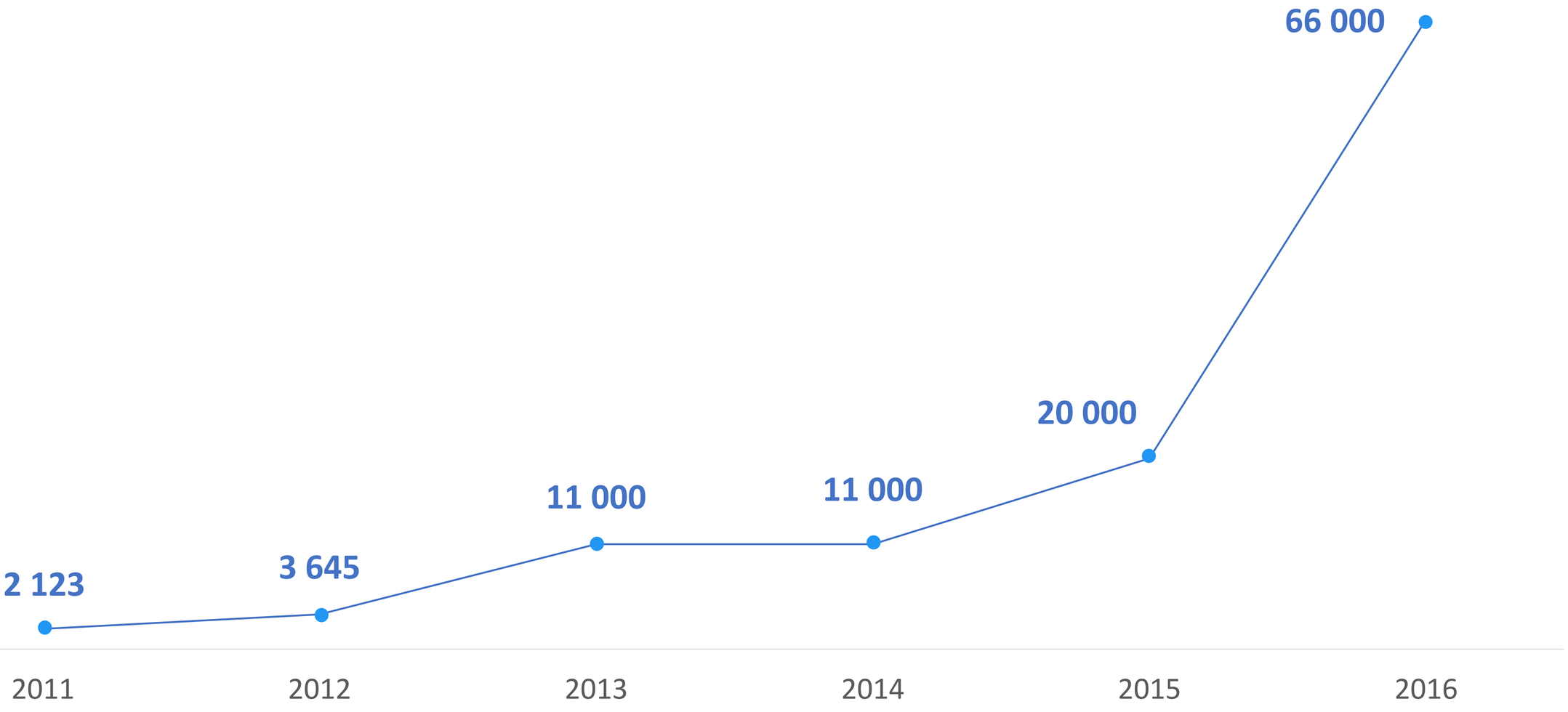
Одна из 7 самых влиятельных компаний в области кибербезопасности по версии Business Insider

Лидер российского рынка по исследованию киберугроз

О нас говорят:

theguardian, Bloomberg, Forbes, REUTERS, Esquire, ПЕРВЫЙ КАНАЛ, РОССИЙСКАЯ ГАЗЕТА, ИЗВЕСТИЯ, ВЕДОМОСТИ, РОССИЯ 1, Коммерсант

Преступления с использованием компьютерных и телекоммуникационных технологий



по данным Генеральной прокуратуры и МВД РФ

Что теряет компания от действий киберпреступников

Деньги

- Перехват покупателей
- Продажа контрафакта, поддельных билетов, полисов, подписок
- Нарушение авторских прав

Доверие

- Хищение персональных данных (фишинг)
- Распространение вредоносных программ с помощью:
  – сайтов
  – мобильных приложений
  – e-mail рассылок
  – объявлений

Репутация

- Информационные атаки на компанию и топ-менеджмент
- Неофициальные аккаунты в социальных сетях

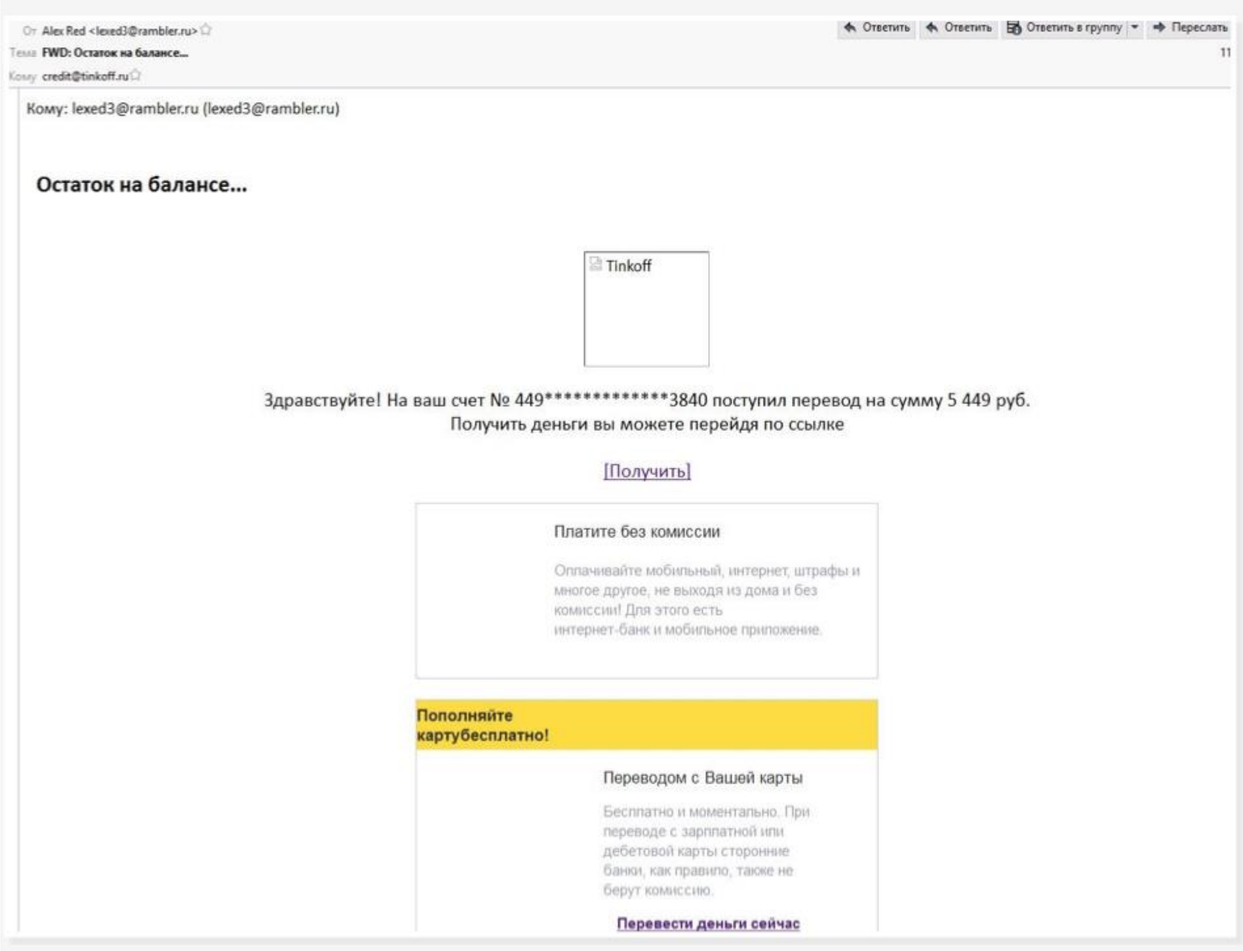
Угрозы бренду в интернете

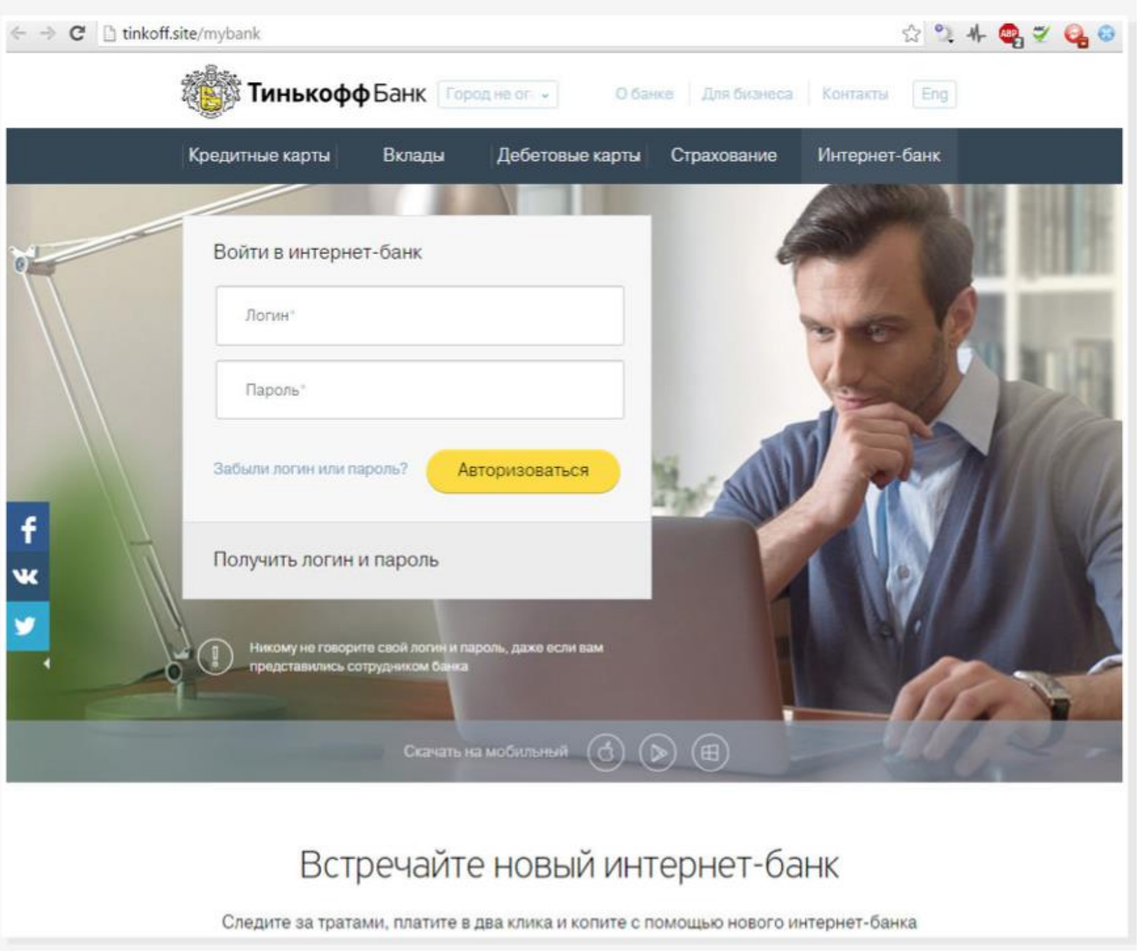
Неправомерное использование бренда, интернет-мошенничество	▪ Сайты-клоны, фишинг, мошеннические сайты ▪ Поддельные мобильные приложения ▪ Неправомерная реклама ▪ Поддельные аккаунты и группы в соцсетях ▪ Ложное партнерство
Информационные атаки, негативные публикации	▪ Направленные бот-атаки против бренда ▪ Негативные отзывы о бренде
Распространение контрафакта и серого импорта	▪ Предложения по продаже контрафактной продукции, серого импорта ▪ Несоблюдения партнёрской политики

Неправомерное использование бренда

Фишинг и сайты-клоны

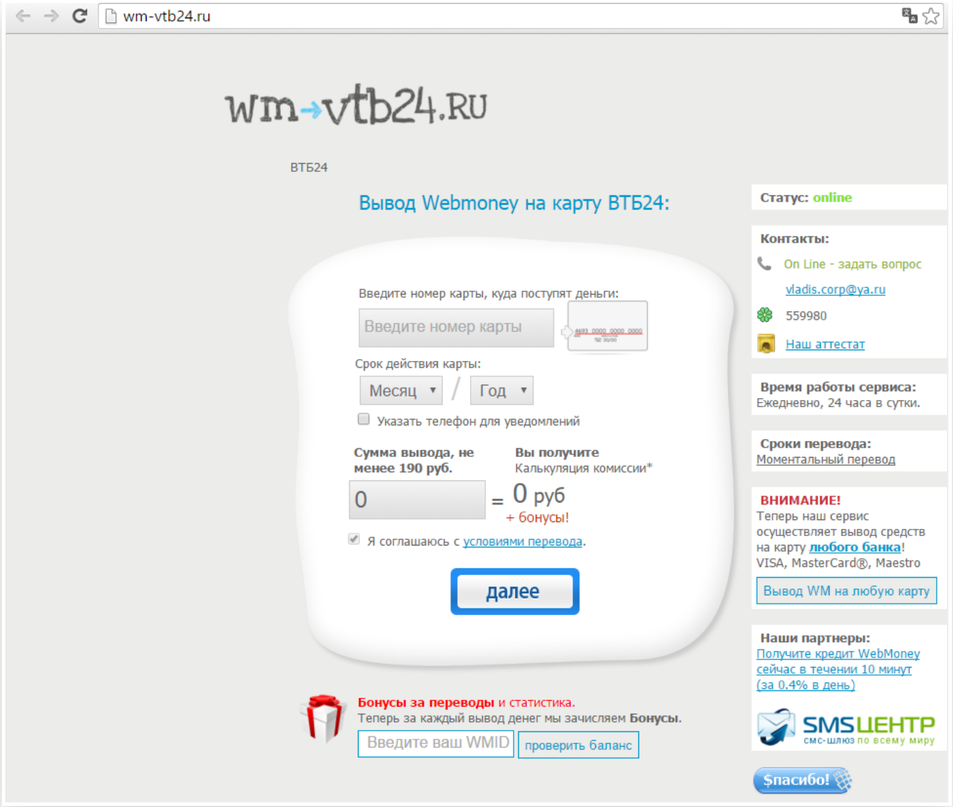
Фишинг в банковской сфере

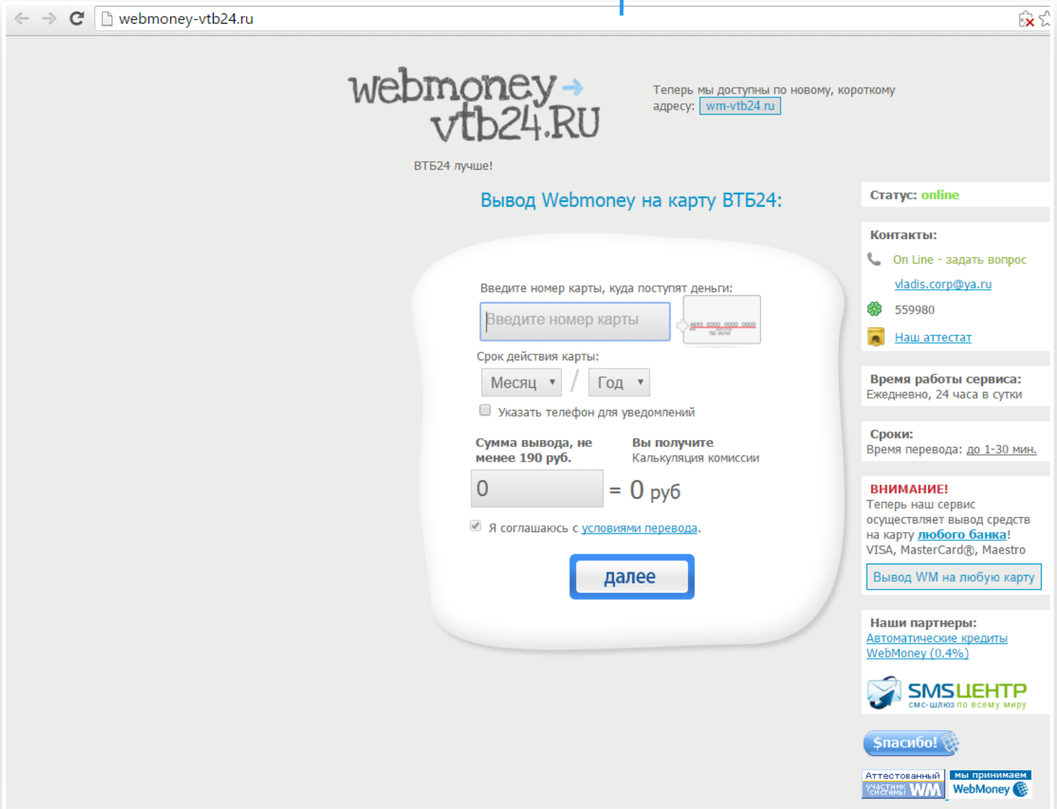




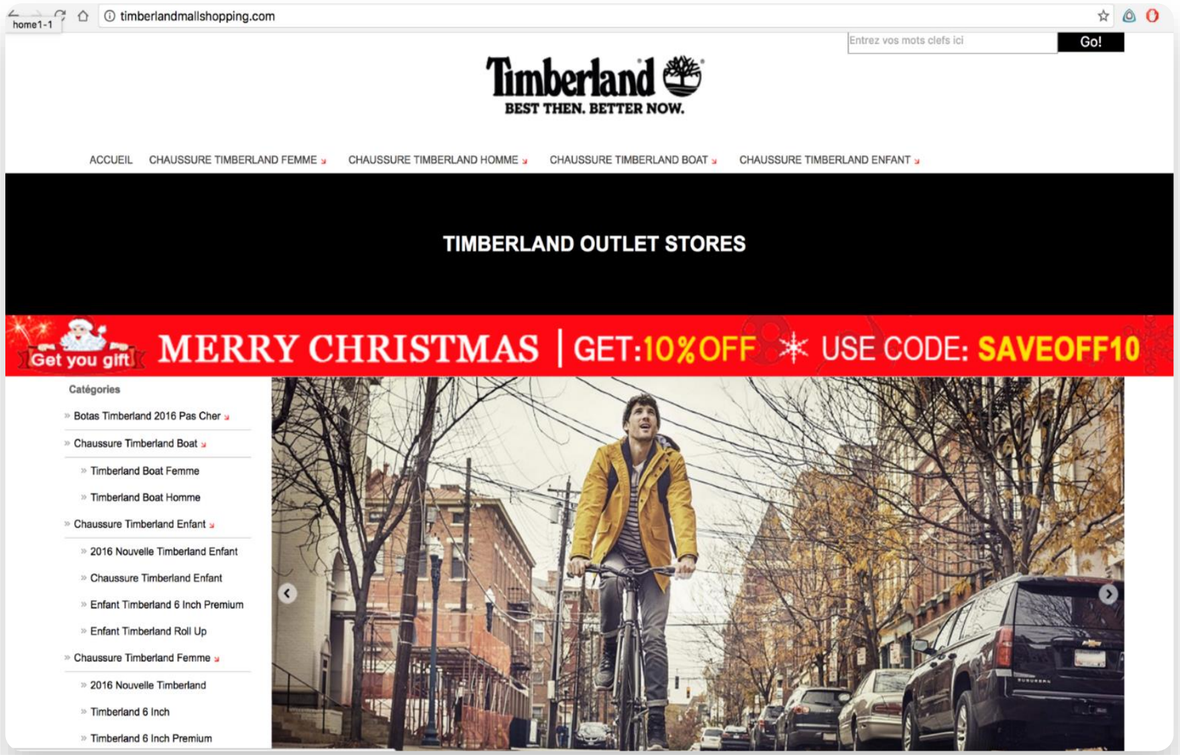
Фишинг в банковской сфере: «удобные» сервисы для пользователей

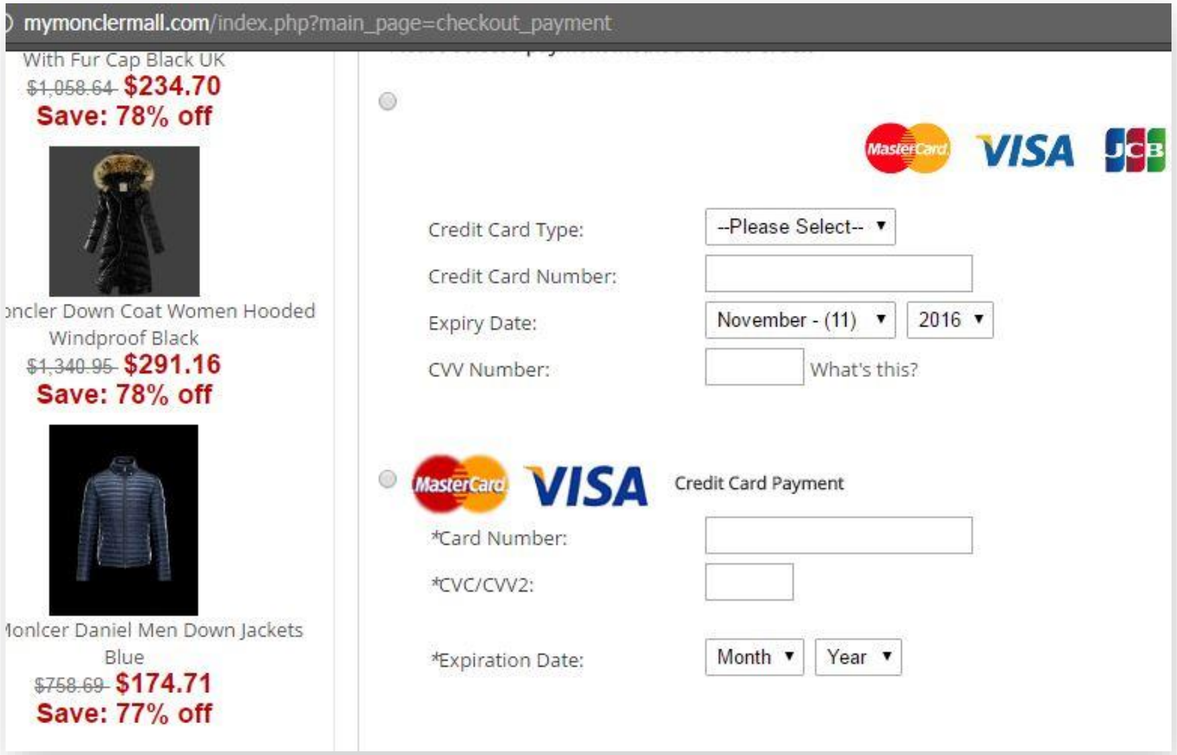
Множество копий
на разных доменах





Фишинговые атаки в ритейле

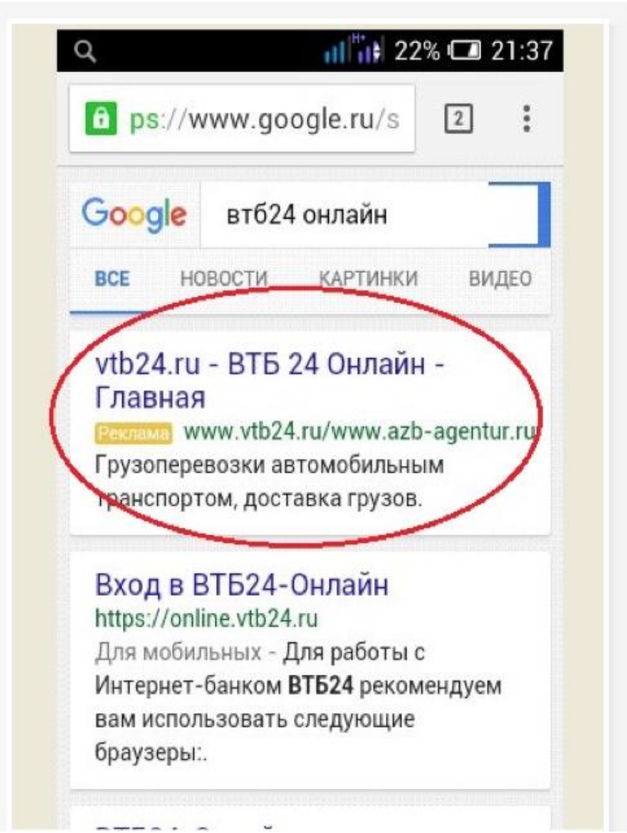


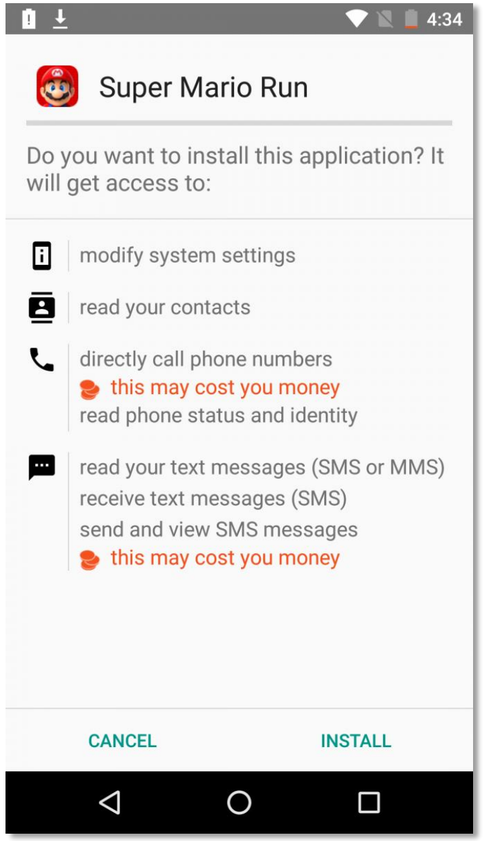


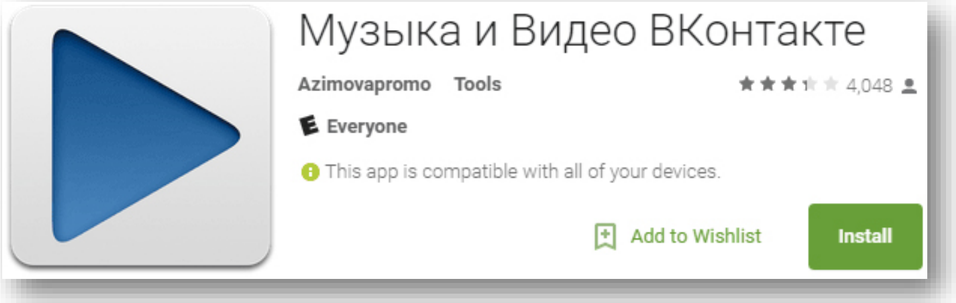
Неправомерное использование бренда

Поддельные мобильные приложения

Поддельные мобильные приложения







Что может банковский троян?

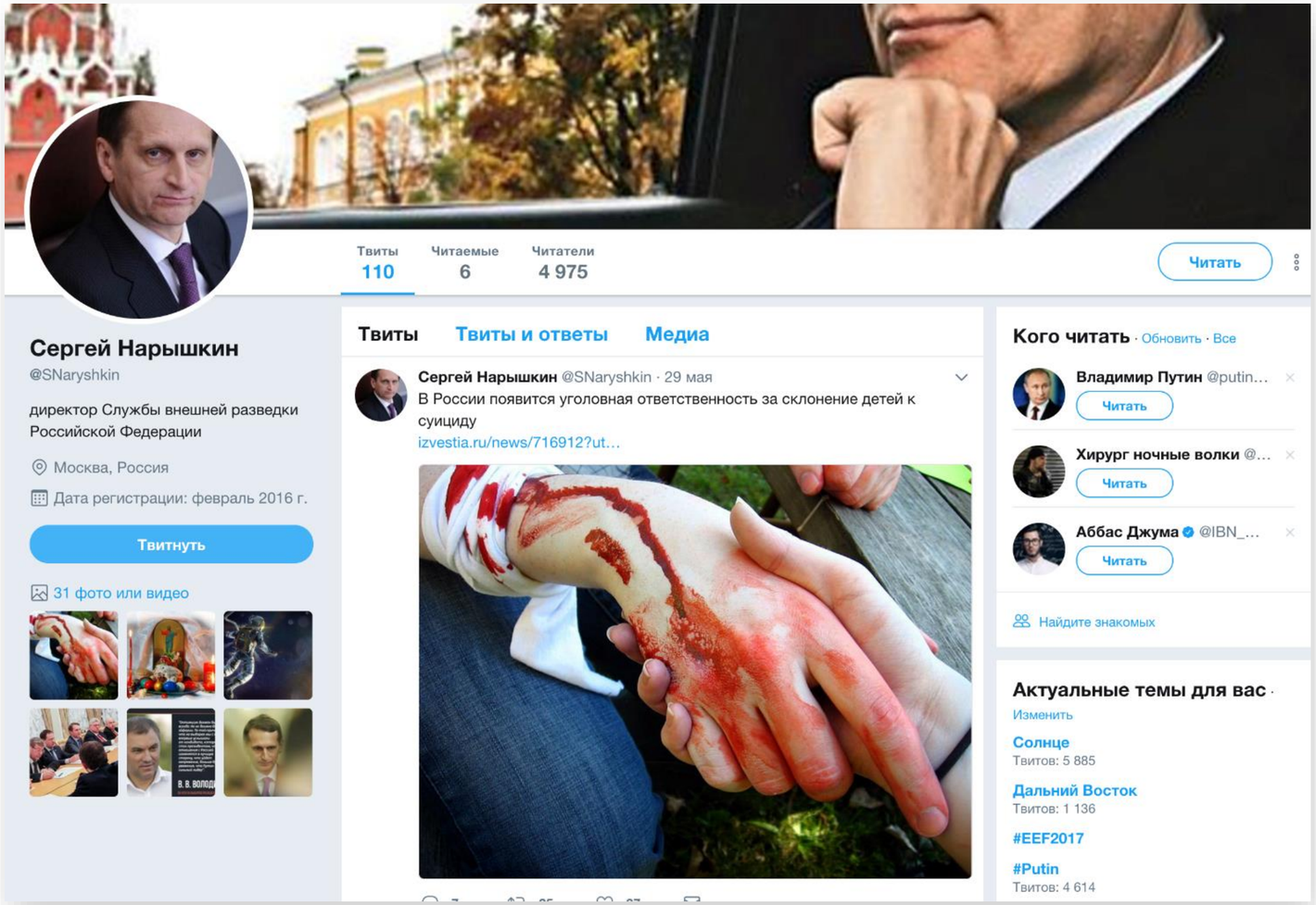
- перехватывать СМС и звонки
- копировать книгу контактов
- следить за местоположением абонента
- активировать камеру
- воровать деньги через онлайн-банк

Неправомерное использование бренда

Поддельные аккаунты и группы в соцсетях

Фейковые профили в соцсетях

Фейковые аккаунты ключевых лиц



Взлом аккаунтов

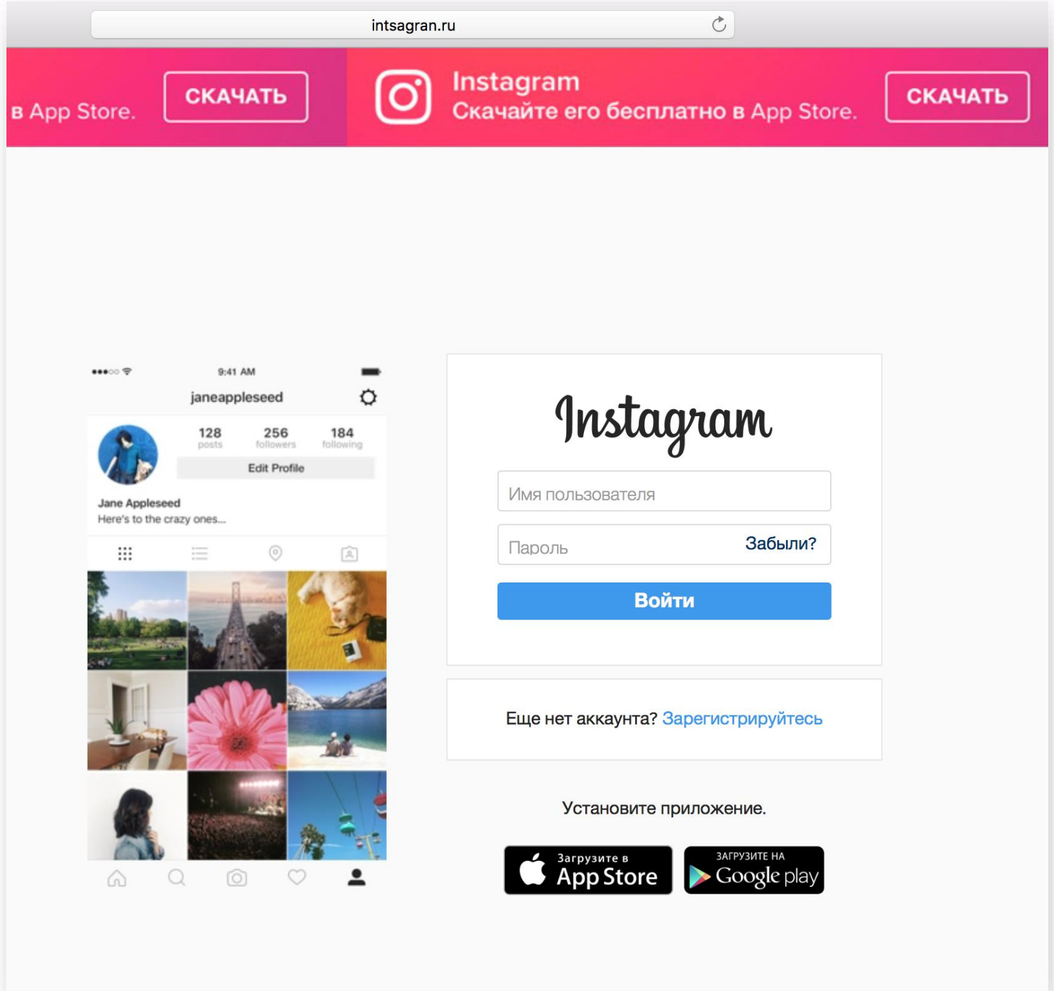
От: Instagram <delivery@instagram-mail-reply.com>
Дата: 25 июня 2017 г., 22:31:18 GMT+3
Кому: <info
Тема: Подтвердите вашу эл. почту.
Ответ-Кому: Instagram <support@mail-config.ru>

Здравствуйте!

Мы увидели подозрительные действия на вашем аккаунте Instagram. Подтвердите ваш адрес электронной почты, чтобы сохранить аккаунт в безопасности и продолжить фотографировать замечательные моменты и делиться ими с миром.

Подтвердите ваш аккаунт

© Instagram, 4 Way, Galeroy Park, CA 92022



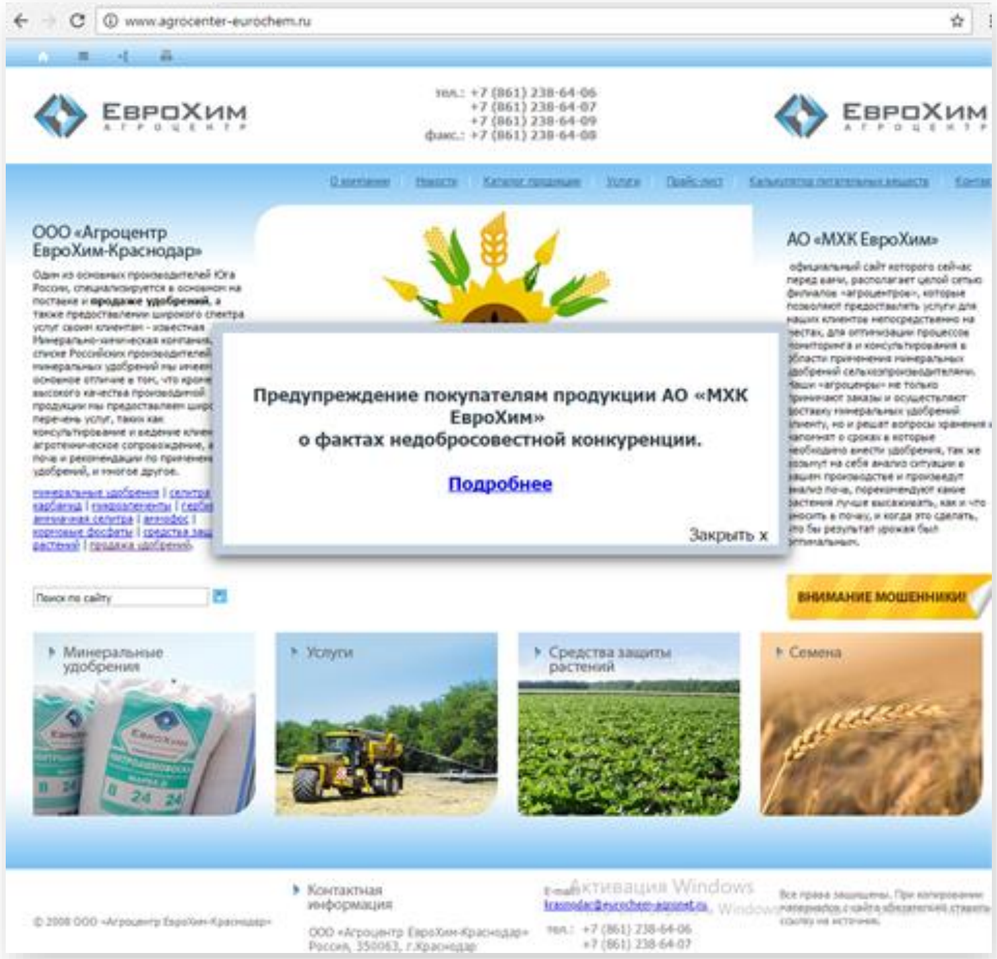
Цели подделки и взлома аккаунтов

- Вымогательство
- Публикация компромата
- Мошенничество в отношении подписчиков
- Целевые атаки

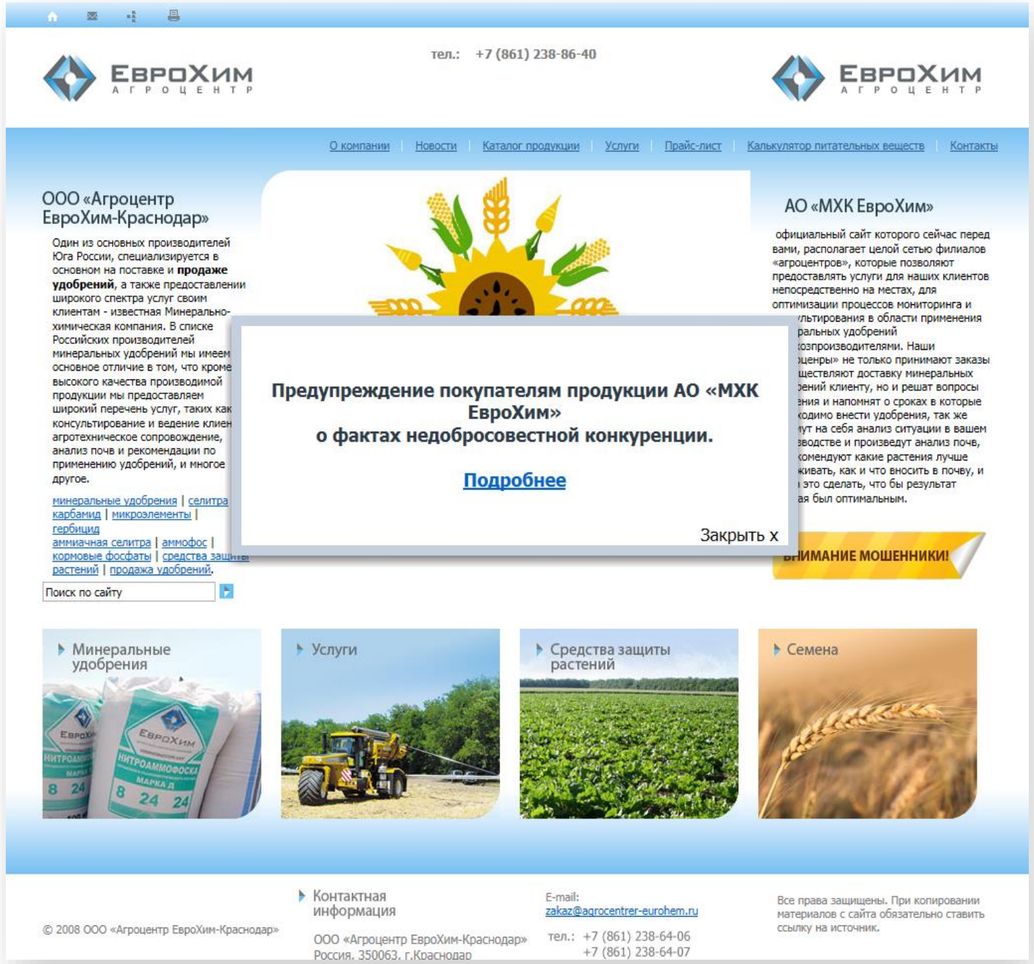
Неправомерное использование бренда

Кейс. Атака на «Еврохим»

Сайт-клон

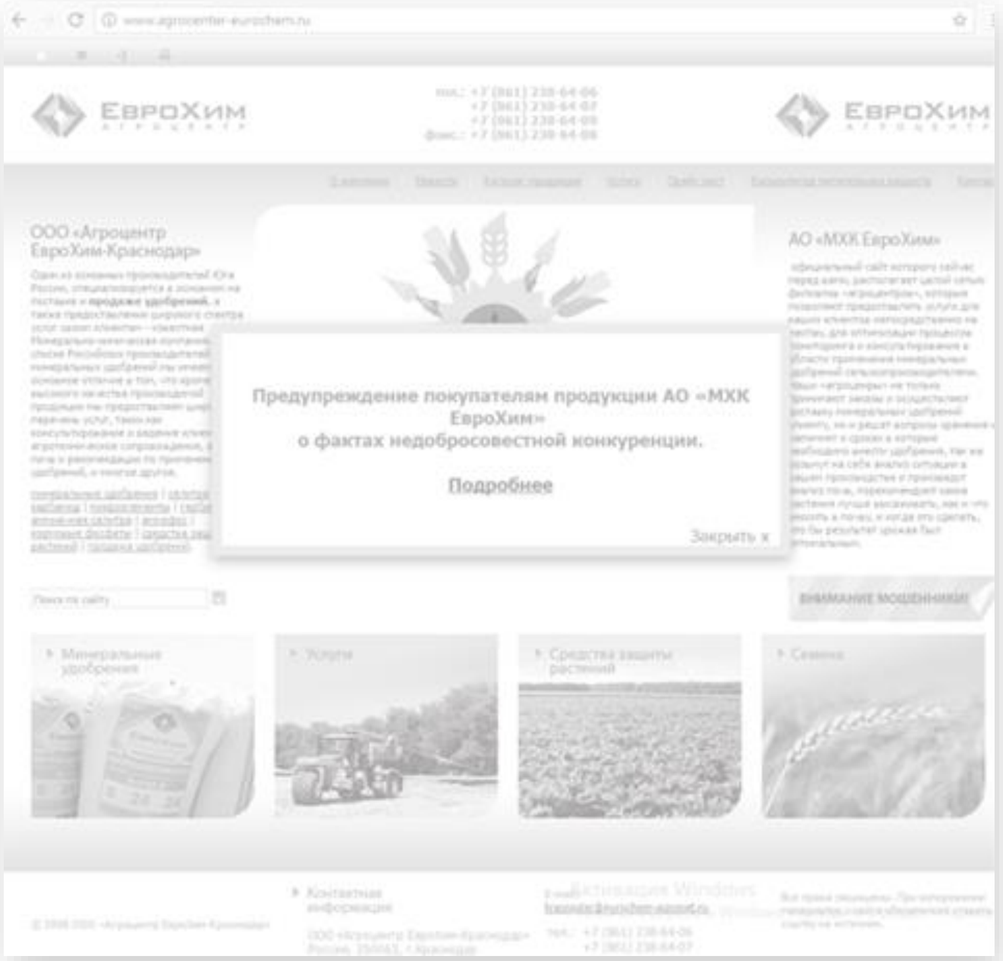


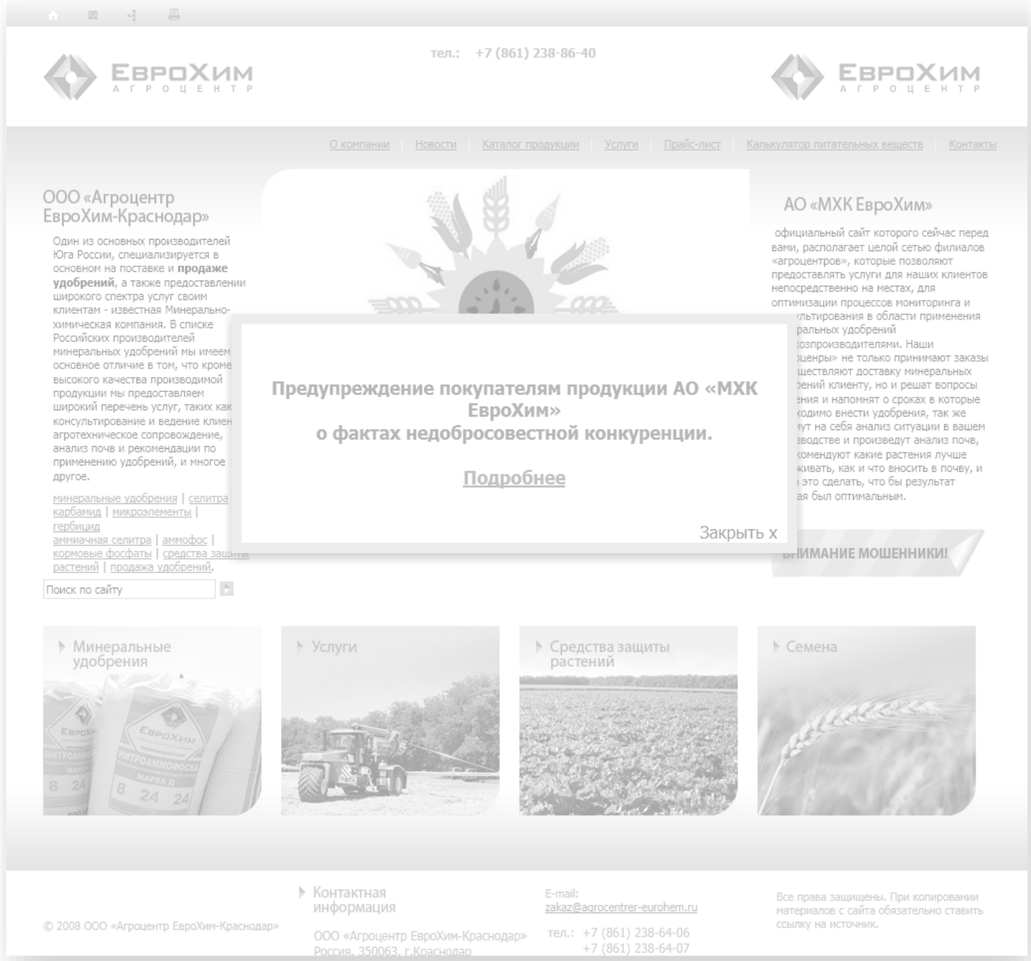
Официальный



Сайт-клон

Сайт-клон





www.agrocenter-eurochem.ru - официальный

www.agrocentrer-eurohem.ru – сайт-клон

Схема работы мошенников: контекстная реклама

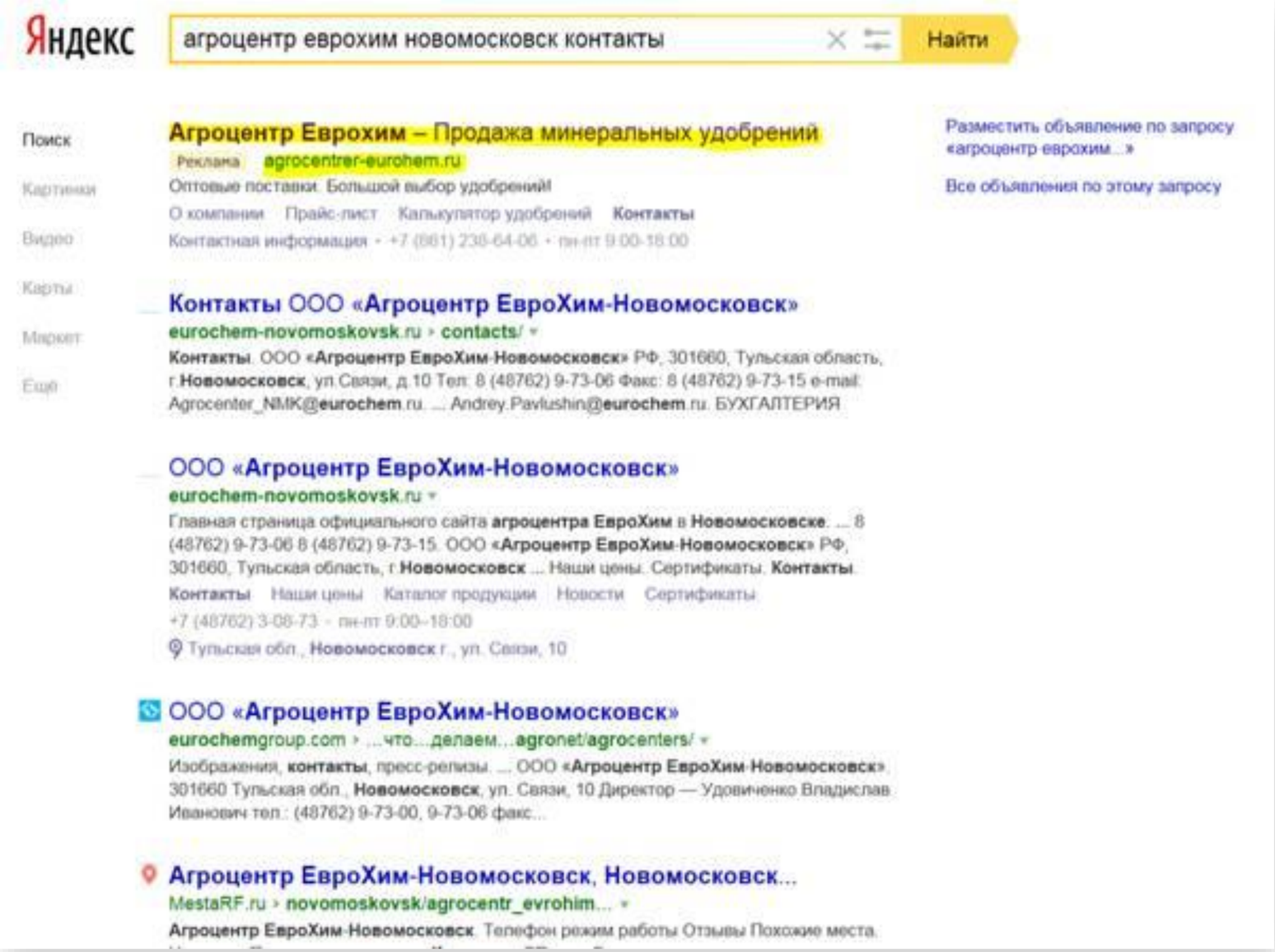


Схема работы мошенников: рассылка КП

ЕвроХим

Общество с ограниченной ответственностью
«Агроцентр ЕвроХим-Краснодар»
ул.Советская 30, г. Краснодар, Россия 301606
Тел. 8 (861) 204 07 75 - Афонин Сергей
agrocentr.14@yandex.ru

№ 2115 от 12.11.2015

Директору ОАО «Концерн Энергомера»

Коммерческое предложение

Направляем это коммерческое предложение с целью начать сотрудничество с Вашей компанией. Предлагаем приобрести минеральные удобрения по следующим ценам:

Вид удобрения	ед. изм.	ООО "Победа", Ставропольский кр., Красногвардейский р-н	ООО "Хлебороб", Ставропольский кр., Петровский р-н	ООО "АПК "Агростандарт", Ставропольский кр., Петровский р-н	ООО "Добровольное", Ставропольский кр., Ипатовский р-н	итого	Цена руб/т.
Ам. селитра	т	0	1 130	0	155,1	1285	13600
КАС-32	т	3 688	550	1 276	748	6262	12130
Аммофос 12:52	т	276	200	236	0	712	31500
карбамид	т	319	110	0	0	429	17250
Диаммофоска 10 26 26	т	0	0	0	48	48	27800
нитроаммофоска 16-16-16	т	0	0	0	105	105	22250
сульфоаммофос 20-20-8	т	0	0	0	144	144	24350
сульфат аммония 21-00-24	т	178	0	0	191	369	10600

Цена указана с учетом НДС и доставки по АПК и после оплаты, изменению не подлежит. Условия оплаты – 100% предоплата. Срок поставки : 15 (пятнадцать) календарных дней после оплаты.

Начальник отдела продаж и маркетинга

Лиманский А.Н.

Схема работы мошенников: подмена адреса отправителя письма

From: Rimma.Timoshkina@eurochem.ru
To: soc@cert-gib.ru
Cc:
Bcc:
Date: Tue, 04 Apr 2017 15:00:30 +0300
Subject: Восстановите сайт!
Добрый день, Просим Вас включить сайт eurochem-novomoskovsk.ru . Так как он является сайтом регионального представительства МХК "ЕвроХим" в городе Новомосковск "ЕвроХим Трейдинг Рус".ОСП Новомосковск, Данный сайт является одним единственным сайтом ОСП Новомосковск. По остальным вопросам можете разговаривать с менеджером отдела маркетинга " Руслан Алиевич Драчев - 89607630498

Заранее спасибо!

--
Тимошкина Римма Николаевна

Ведущий специалист отдела продаж

ООО "ЕвроХим Трейдинг Рус"

ОСП в г.Новомосковск

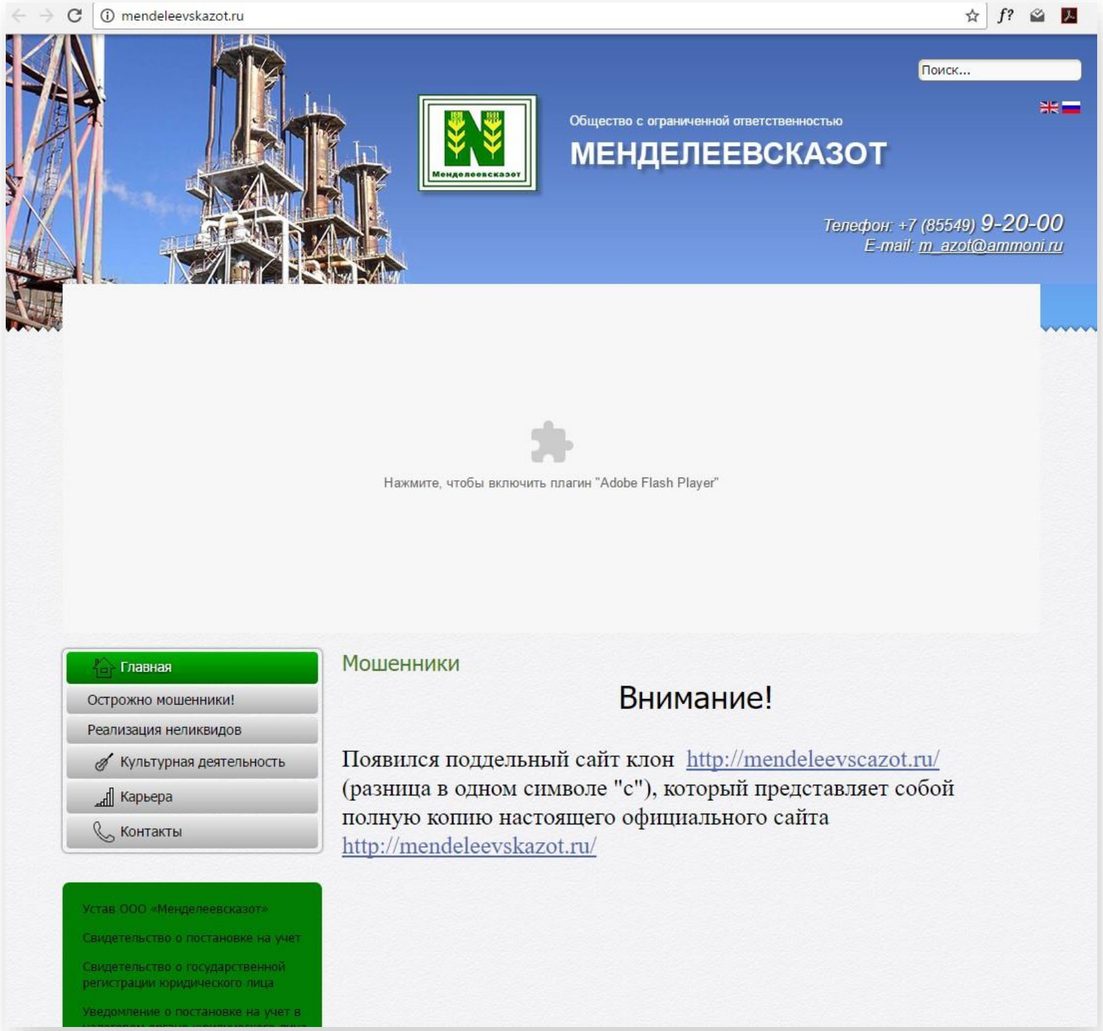
телефон (48762) 97-306,

факс (48762) 97-315

e-mail:Rimma.Timoshkina@eurochem.ru

www:www.eurochem.ru

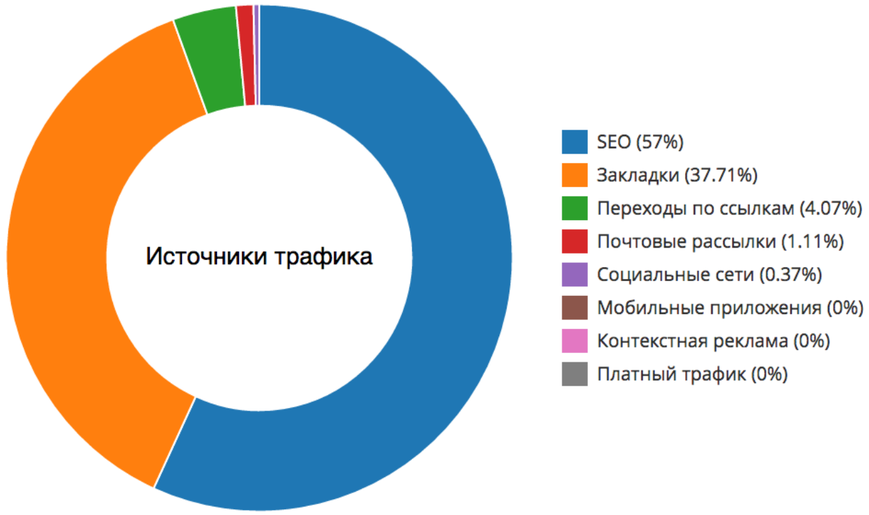
Сайт-клон Менделеевсказота

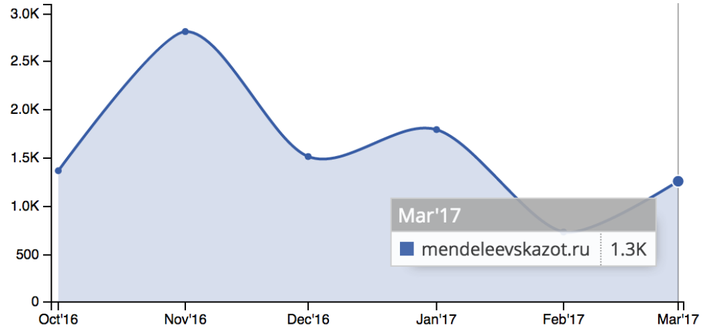


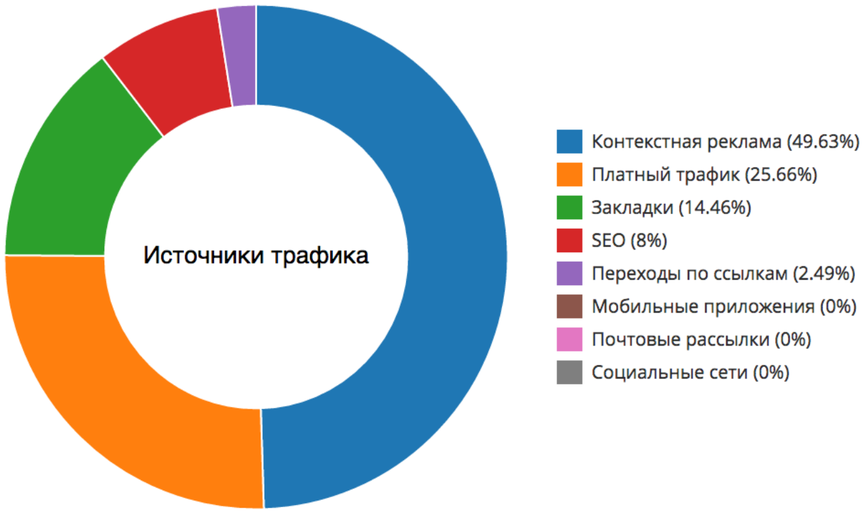
Официальный

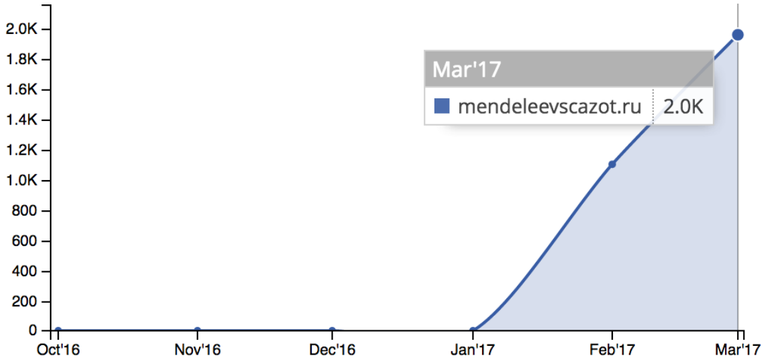
Сайт-клон

Продвижение сайтов-клонов









Официальный ресурс
www.mendeleevskazot.ru

Сайт-клон
www.mendeleevscazot.ru

Про ущерб

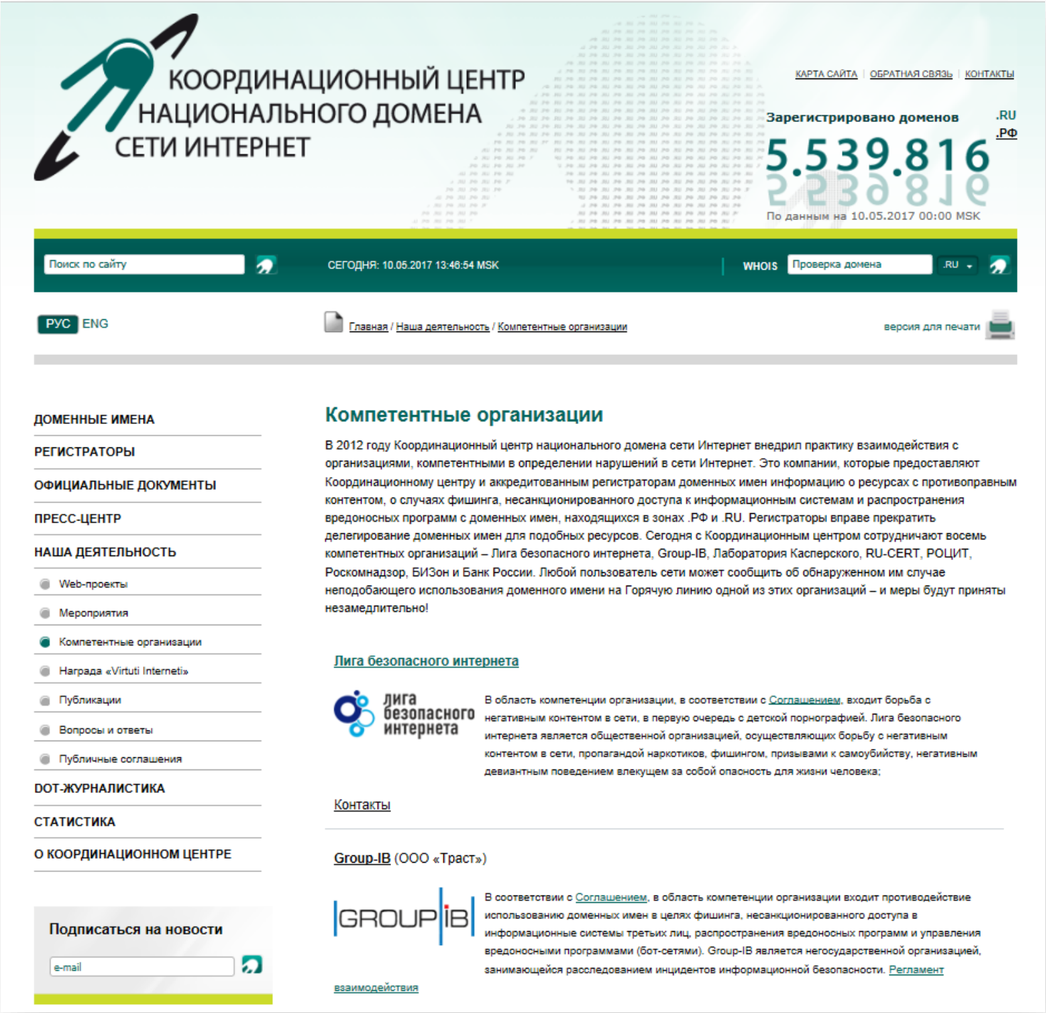
За последние два сезона фермеры из-за мошенников потеряли несколько миллиардов рублей

Дмитрий Стрежнев, генеральный директор компании «Еврохим»

Анализируйте мошеннические сайты: один сайт может вывести на десятки других связанных с ним сайтов

1. Превентивно регистрируйте схожие доменные имена
2. Постоянно мониторьте доменные имена, поисковую выдачу, базу фишинговых ресурсов
3. Отслеживайте способы их продвижения: контекстную рекламу, посты в соцсетях и мессенджерах
4. Выявляйте аналогичные мошеннические сайты при помощи анализа связей и аффилированности сайтов
5. Блокируйте мошеннические ресурсы: обращайтесь к компаниям со специальной компетенцией по блокировке сайтов

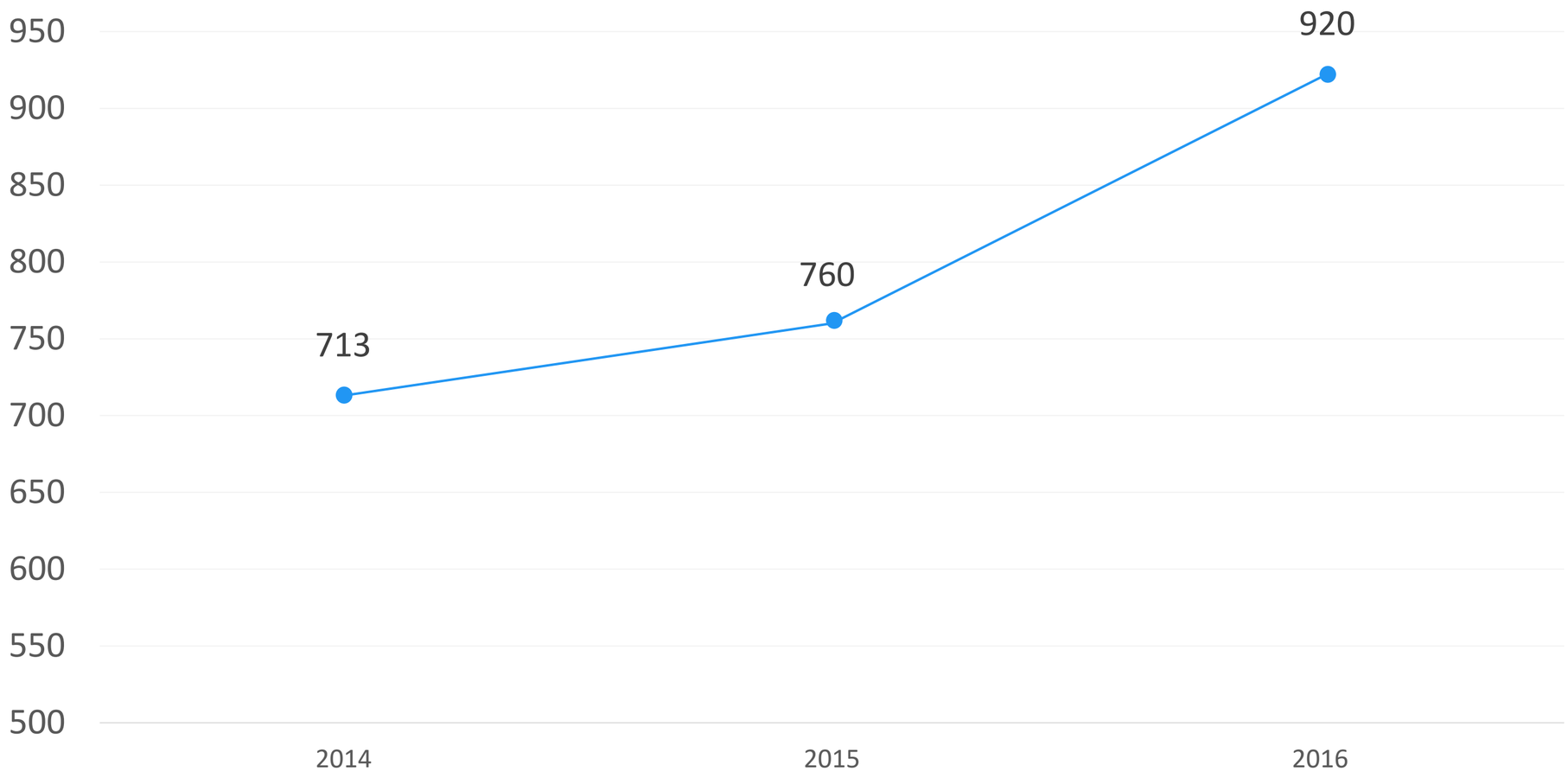
Компетентные организации



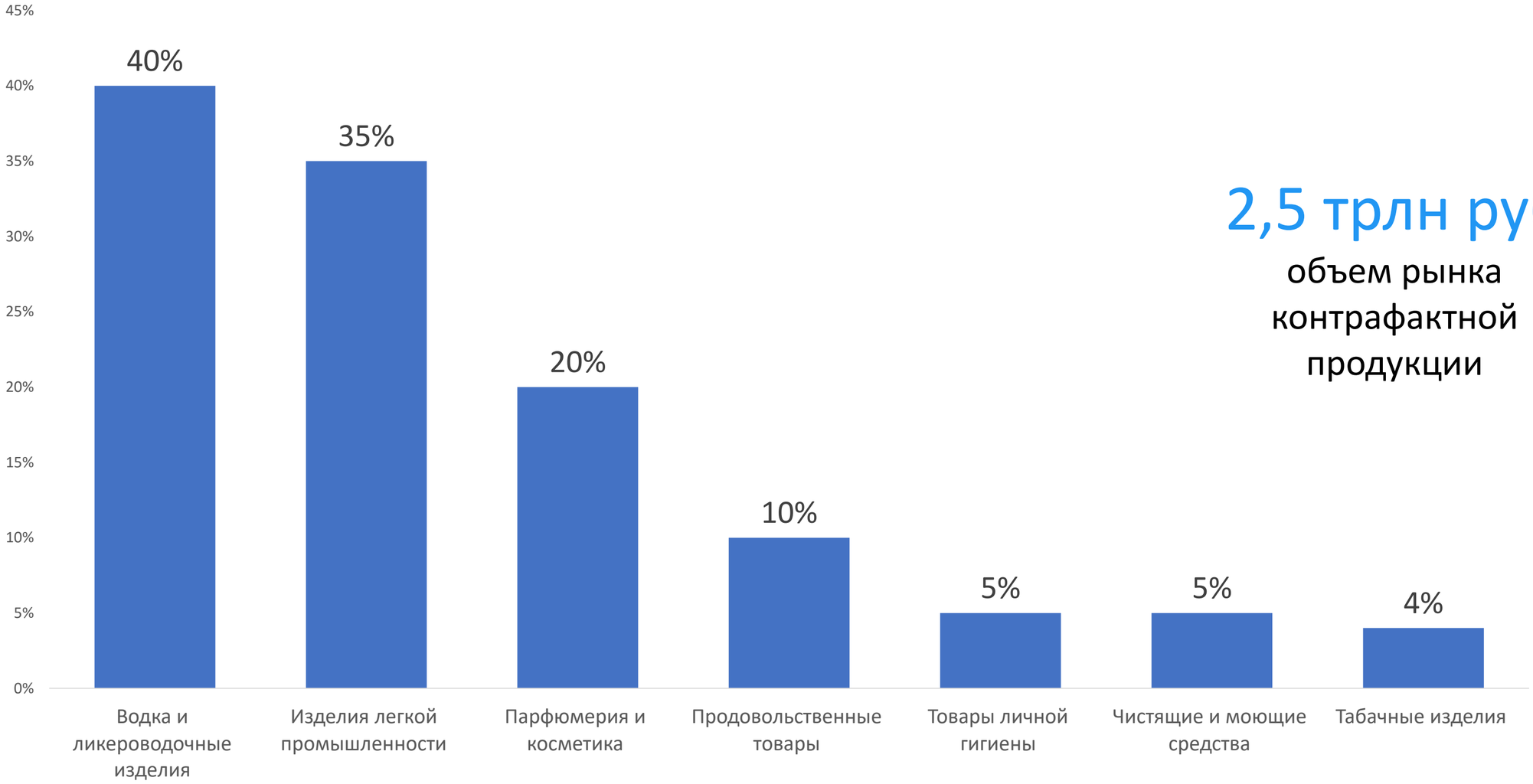
https://cctld.ru/ru/safety/competent/

Распространение контрафакта и серого импорта

Объемы ecommerce России, млрд. руб



Доли незаконного оборота по товарным рынкам в РФ

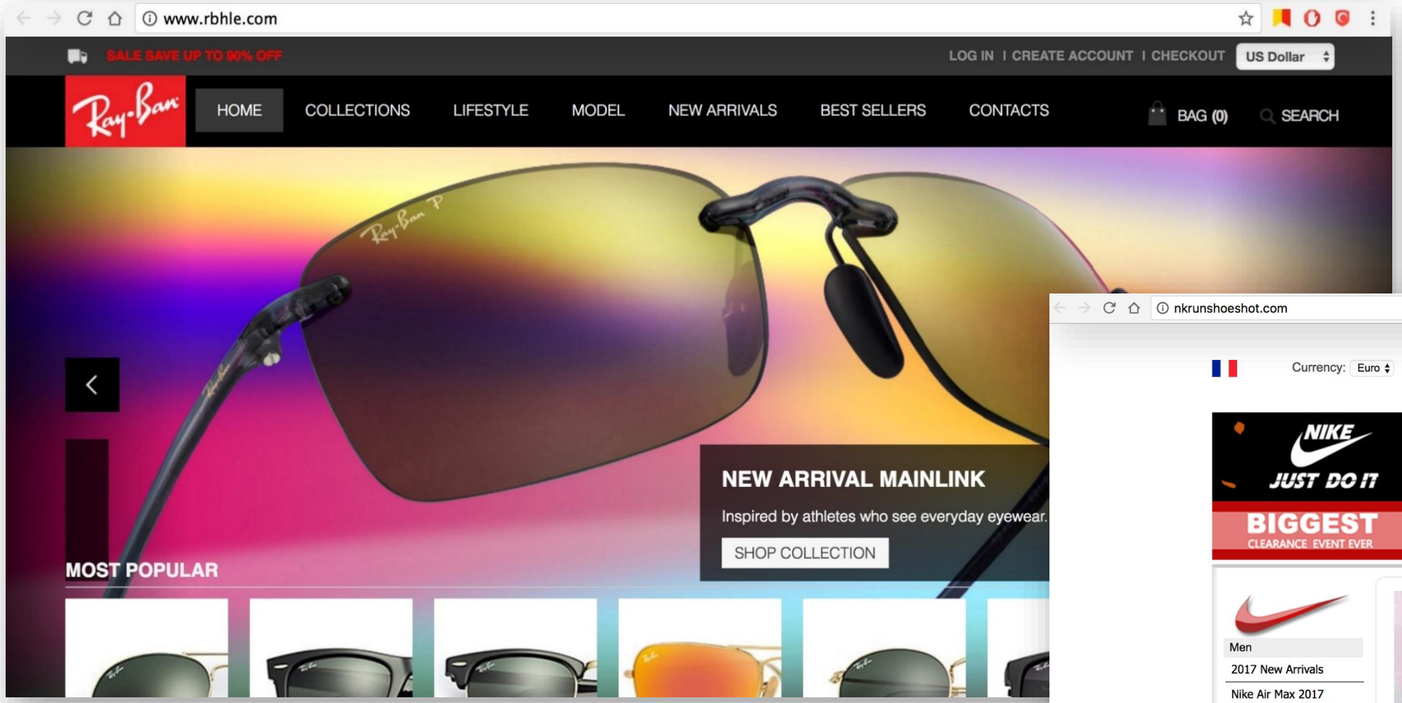


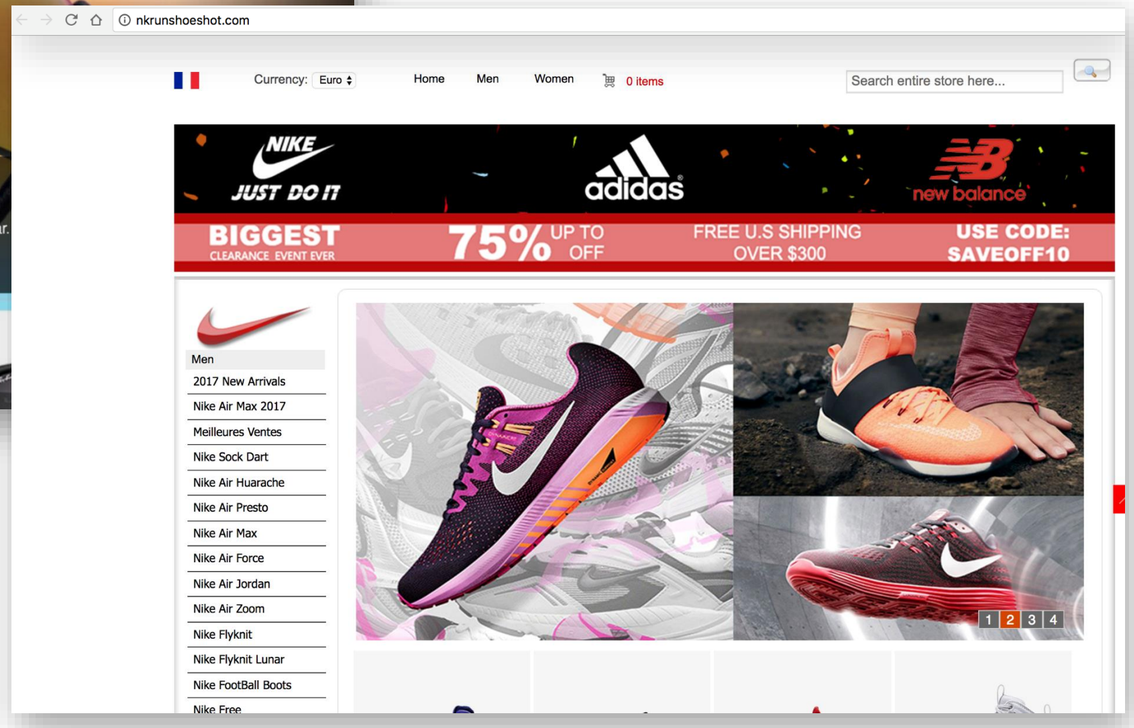
2,5 трлн руб

объем рынка контрафактной продукции

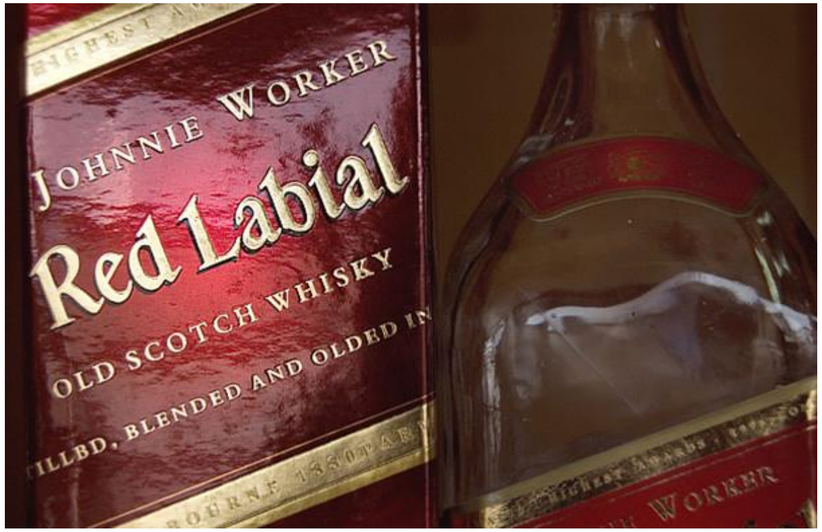
Данные НИУ-ВШЭ, 2016

Распространение контрафакта. Размытие бренда

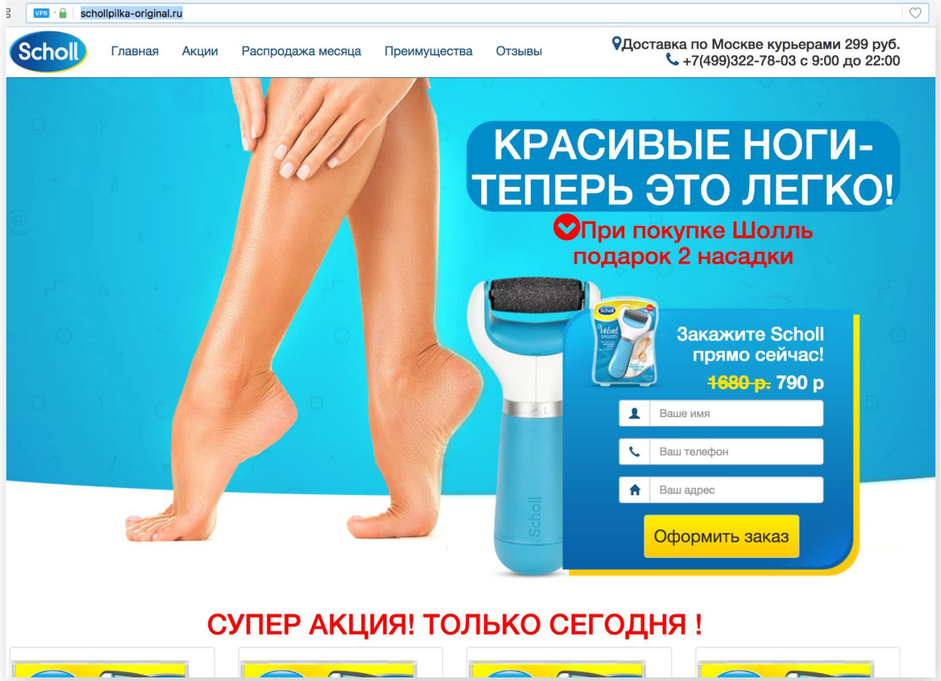


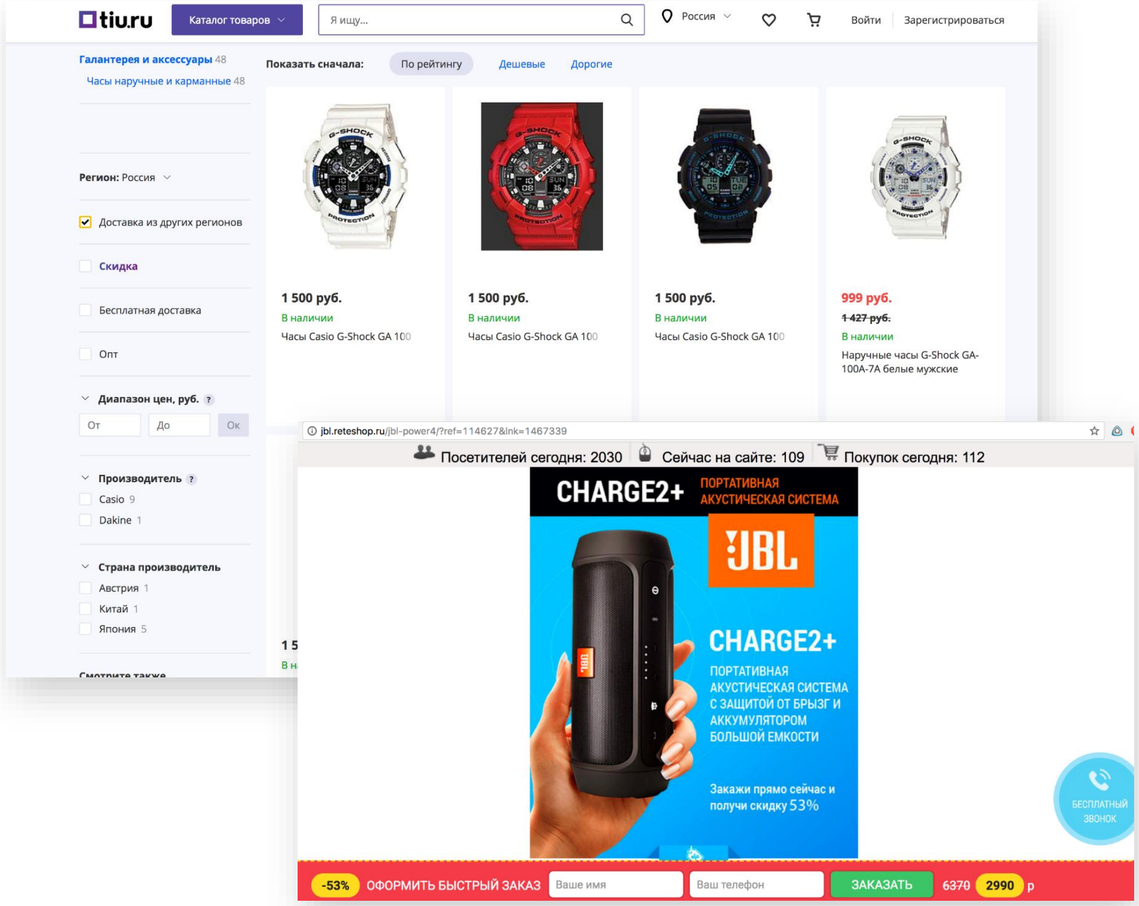


Креатив в контрафакте



Распространение контрафакта





За год по одному бренду Group-IB блокирует объявления о продаже контрафактной продукции на сумму более

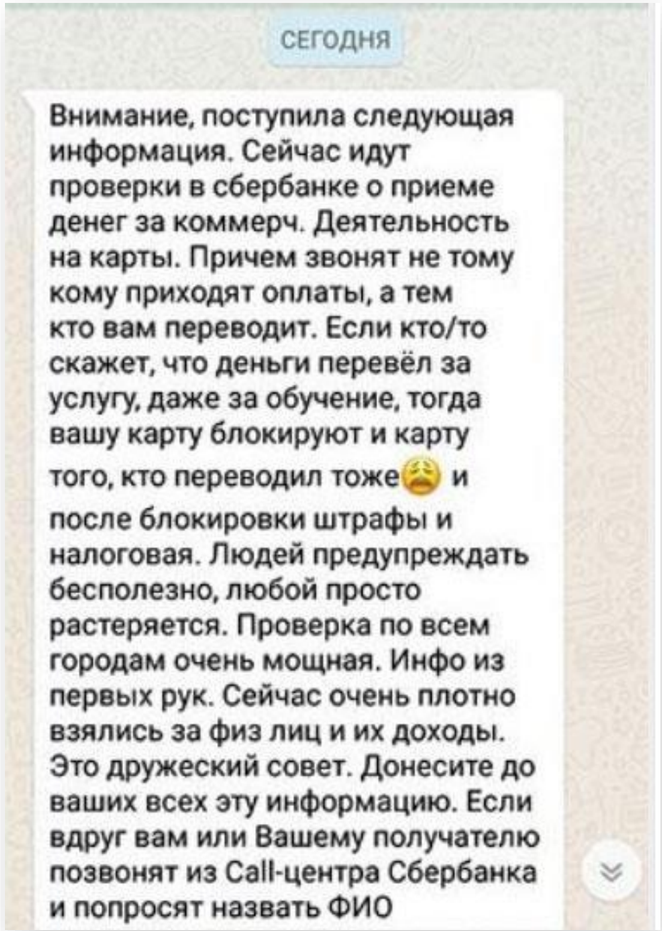
400 млн руб

Не перегружайте ваших юристов - используйте технологии мониторинга и обнаружения контрафакта в онлайне

1. Постоянно мониторьте упоминания своего бренда в интернет-магазинах, агрегаторах, доменных именах, досках объявлений, соцсетях
2. Блокируйте сайты и удаляйте объявления:
   - Блокировка сайтов через регистраторов и хостинг-провайдеров
   - Удаление предложений через администраторов интернет-магазинов, соцсетей, досок объявлений, агрегаторов, поисковых систем, магазинов приложений, рекламных сетей
   - Договоренность с реальными владельцами ресурсов о прекращении незаконного использования бренда
3. При необходимости обращайтесь в суд

Информационные атаки

Пример информационной атаки



Атака на «Сбербанк»

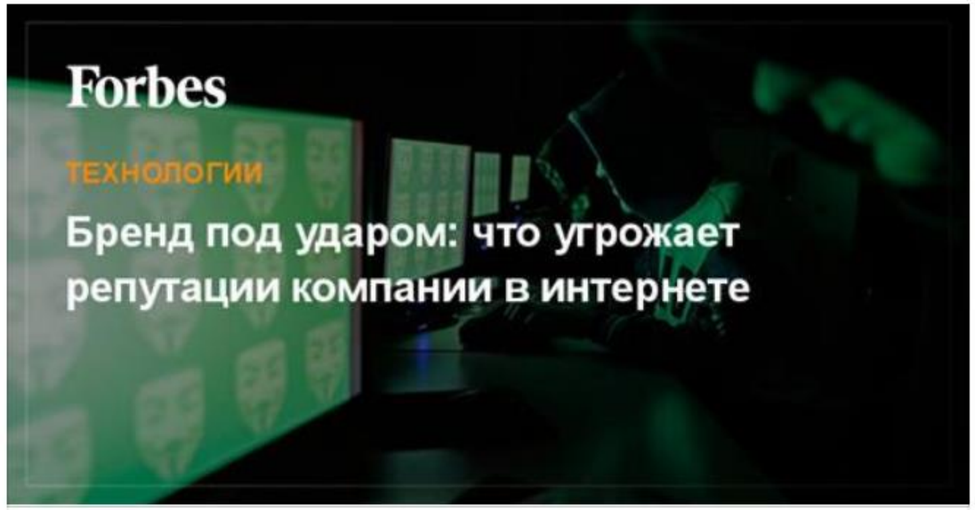
Атака на «Приватбанк»

Как бороться с информационными атаками

Выявляйте информационные атаки на этапе их зарождения

1. Отслеживайте упоминания своего бренда в постах в соцсетях
2. Анализируйте связи между ними – это возможно при помощи технологий Big Data
3. Оперативно принимайте контрмеры

Статьи о мошенничествах с использованием бренда



Бренд под ударом: что угрожает репутации компании в интернете

Какие технологии в сфере кибербезопасности могут защитить доброе имя компании

FORBES.RU

Атака клонов: как работают схемы с фейковыми сайтами «Роснефти» и других крупных компаний

Злоумышленники создают копии сайтов российских корпораций, чтобы заключать контракты от их имени. Средний ущерб от такой атаки — от 1,5 млн рублей

FORBES.RU

http://www.forbes.ru/tehnologii/337375-brend-pod-udarom-chto-ugrozhaet-reputacii-kompanii-v-internete

http://www.forbes.ru/biznes/342465-ataka-klonov-kak-ustroena-moshennicheskaya-shema-s-feykovymi-saytami

Что угрожает вашему бренду в интернете

Тип	*Уровень угрозы*	*Комментарий*
Неавторизованная торговля	Высокий	Более 1 200 предложений было обнаружено на сайтах бесплатных объявлений и форумах
Социальные сети	Высокий	Выявлено более 800 неофициальных сообществ и более 200 аккаунтов в различных социальных сетях, использующих бренд заказчика. Суммарное количество подписчиков составляет более 200 000 человек
Реклама	Средний	Обнаружено более 50 случаев использования бренда заказчика в рекламе
Доменные имена	Высокий	Обнаружено более 150 доменов, которые могут представлять угрозу для заказчика

Отправьте заявку на bp@group-ib.ru с темой «Аудит бренда» и получите объективный анализ угроз и рекомендации по их устранению. Это бесплатно

Дмитрий Русаков
rusakov@group-ib.com
+7 915 315 68 25

Предотвращаем и расследуем киберпреступления с 2003 года

www.group-ib.ru
blog.group-ib.ru
bp@group-ib.ru
+7 495 984 33 64
twitter.com/groupib
facebook.com/group-ib
t.me/group_ib
instagram.com/group_ib