V ВСЕРОССИЙСКАЯ КОНФЕРЕНЦИЯ

ВЗГЛЯД В **ЦИФРОВОЕ** БУДУЩЕЕ

Ростелеком

ИКТ ИНФРАСТРУКТУРА ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ



Тенденции развития киберугроз, направленных на органы государственной власти



О Group-IB

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 и INTERPOL

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

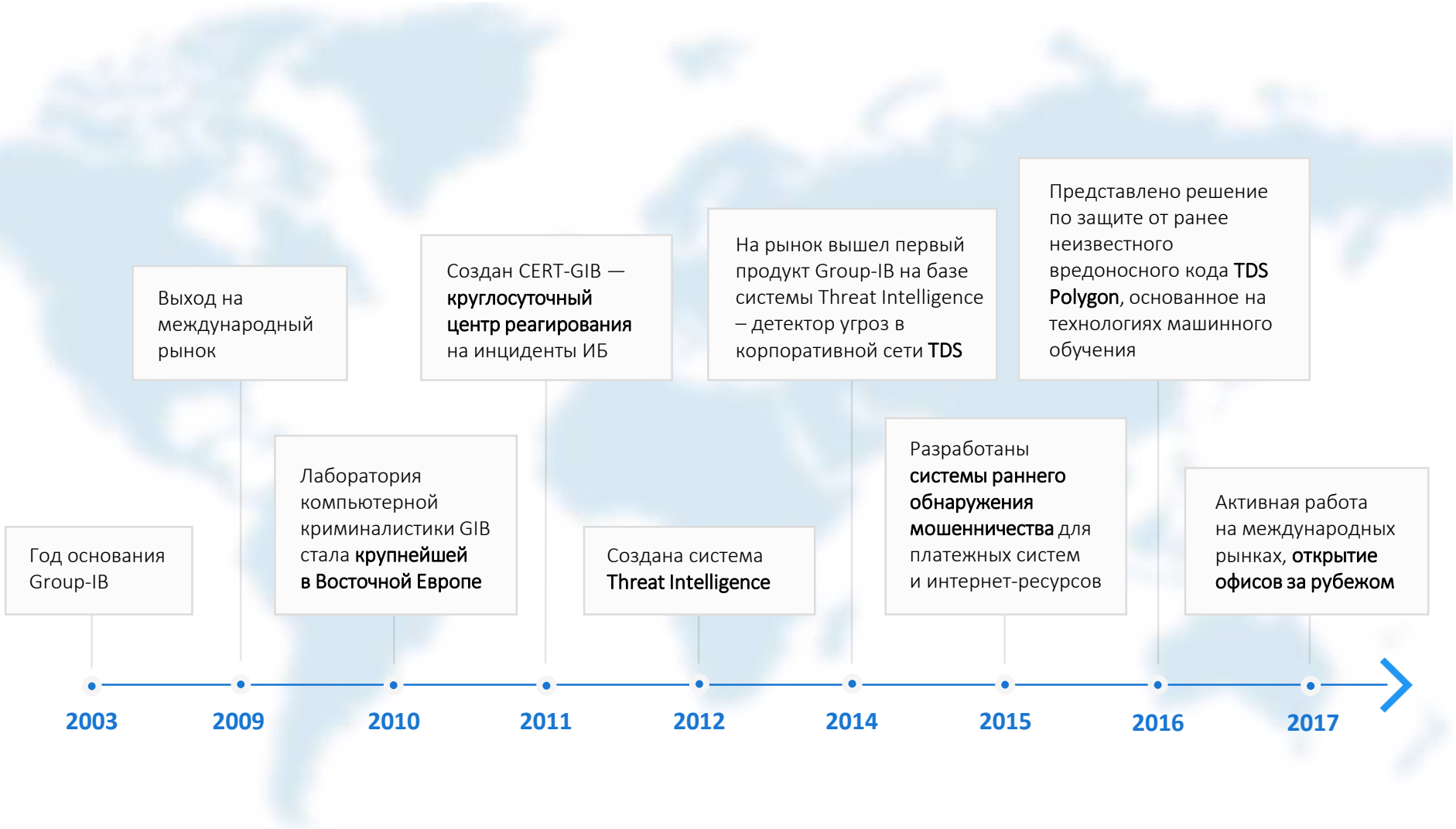
Одна из 7 самых влиятельных компаний в области кибербезо-пасности по версии Business Insider

Лидер российского рынка по исследованию киберугроз

О нас говорят: theguardian Bloomberg Forbes REUTERS Esquire

ПЕРВЫЙ КАНАЛ РОССИЙСКАЯ ГАЗЕТА ИЗВЕСТИЯ ВЕДОМОСТИ РОССИЯ 1 Коммерсантъ

История компании



Многолетний опыт Group-IB воплощен в системе раннего обнаружения киберугроз — линейке высокотехнологичных продуктов, основанной на самых актуальных данных и глубоком анализе реальных хакерских атак.

210+
сотрудников

40%
разработчиков

27
средний возраст

45 000
часов реагирования

Центр реагирования CERT-GIB

CERT-GIB (Computer Emergency Response Team) — центр круглосуточного реагирования на инциденты информационной безопасности

- Мониторим появление фишинговых ресурсов, распространение вредоносного ПО, торговлю контрафактом
- Оказываем полную юридическую поддержку на всех этапах реагирования и расследования
- Оперативно блокируем опасные сайты в доменах .RU, .РФ, и еще более 2000 доменных зон
- Работаем по всему миру: через сеть партнеров, контакт с хостинг-провайдерами и регистраторами доменных имен

Ростех, одна из крупнейших российских госкорпораций, выбрала Group-IB в качестве партнера для создания собственного CERT RT-Inform

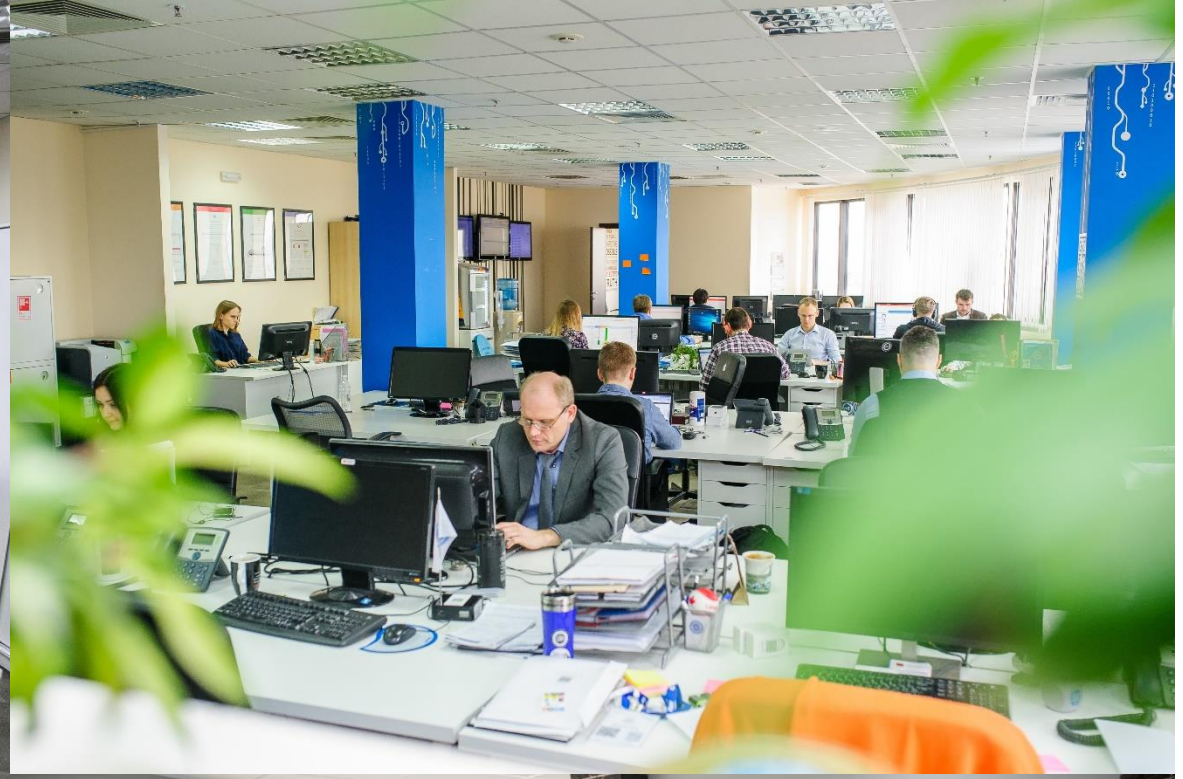
Компетентная организация Координационного центра национального домена сети Интернет и Фонда развития интернета

Аккредитованный член международных сообществ FIRST и Trusted Introducer

Партнер IMPACT – международного партнерства по противодействию киберугрозам

Авторизован Университетом Карнеги, официально использует торговую марку CERT


Moscow
16:08 47

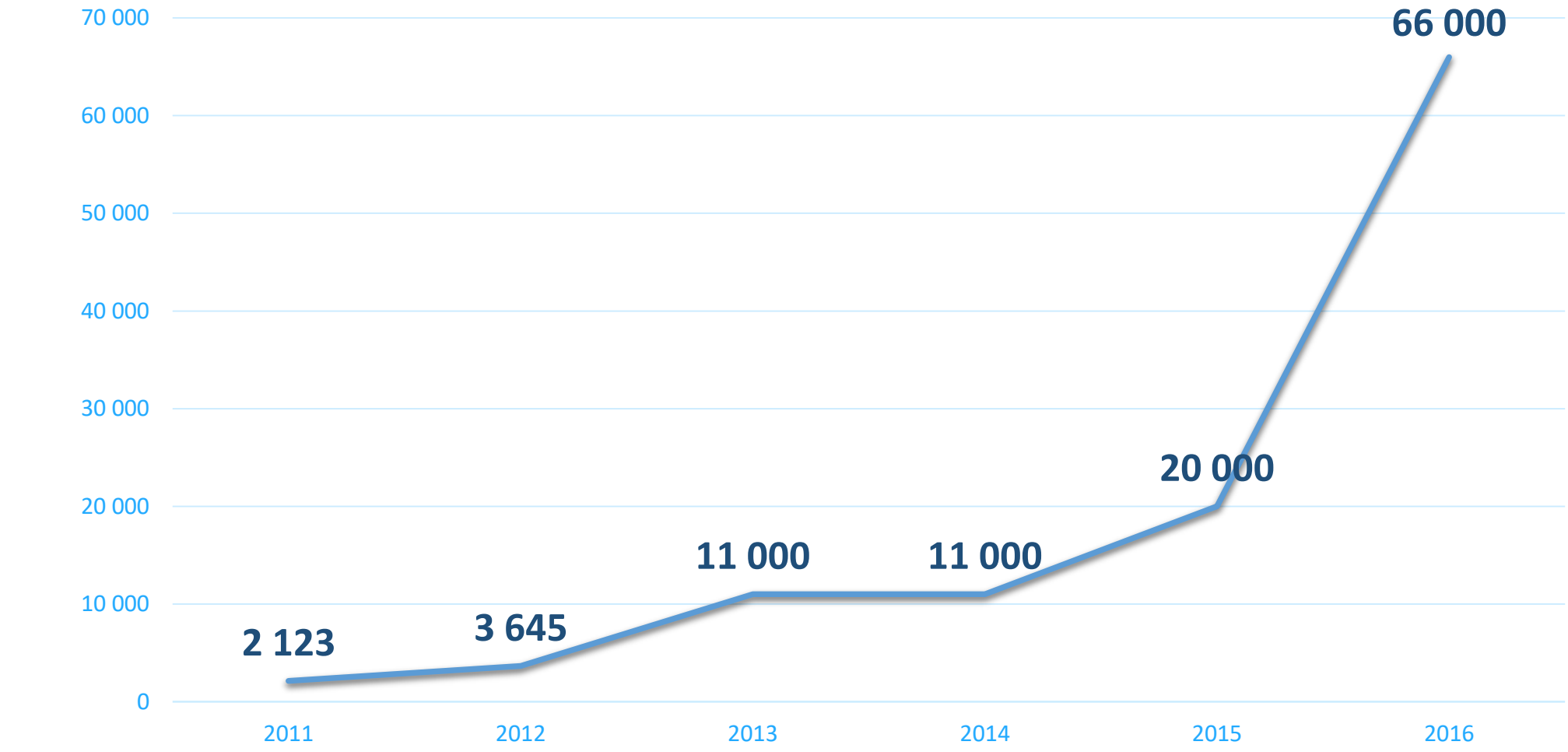



Владимирская
область




РОДИНА СЛЫШИТ!

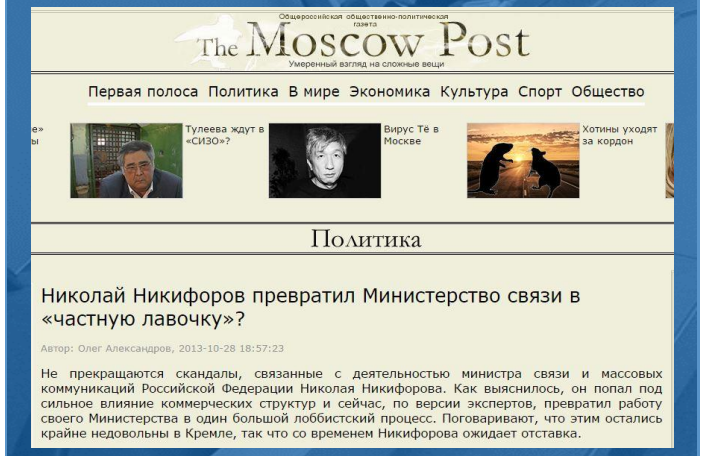
Преступления совершенные с использованием компьютерных и телекоммуникационных технологий



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Мошенничество с использованием названия государственного учреждения

Мы фиксировали создание мошеннических площадок с использованием названий крупных государственных компаний России и органов государственной власти



С целью вымогательства

Преступники могут регистрировать доменные имена, созвучные с доменами сервисов Портала электронного правительства, размещая на них копии официальных сайтов.

После этого мошенники распространяют уведомления при помощи почтовых рассылок и заражают устройство пользователя.

Последствие - вирус шифрует файлы документов и таблиц, за расшифровку данных злоумышленники требуют деньги.

С целью осуществления хищений

По аналогичной схеме может создаваться сайт, на котором будет выложен вредоносный код, делается рассылка писем от имени сервисов Портала Госуслуг по юридическим лицам или физическим лицам.

Последствие – злоумышленники получают доступ к компьютеру жертвы и производят хищения через системы онлайн банка (юридические, физические лица).

С целью нанесения репутационного ущерба организации и его руководству

В СМИ распространяются ложные сведения об органе государственной власти

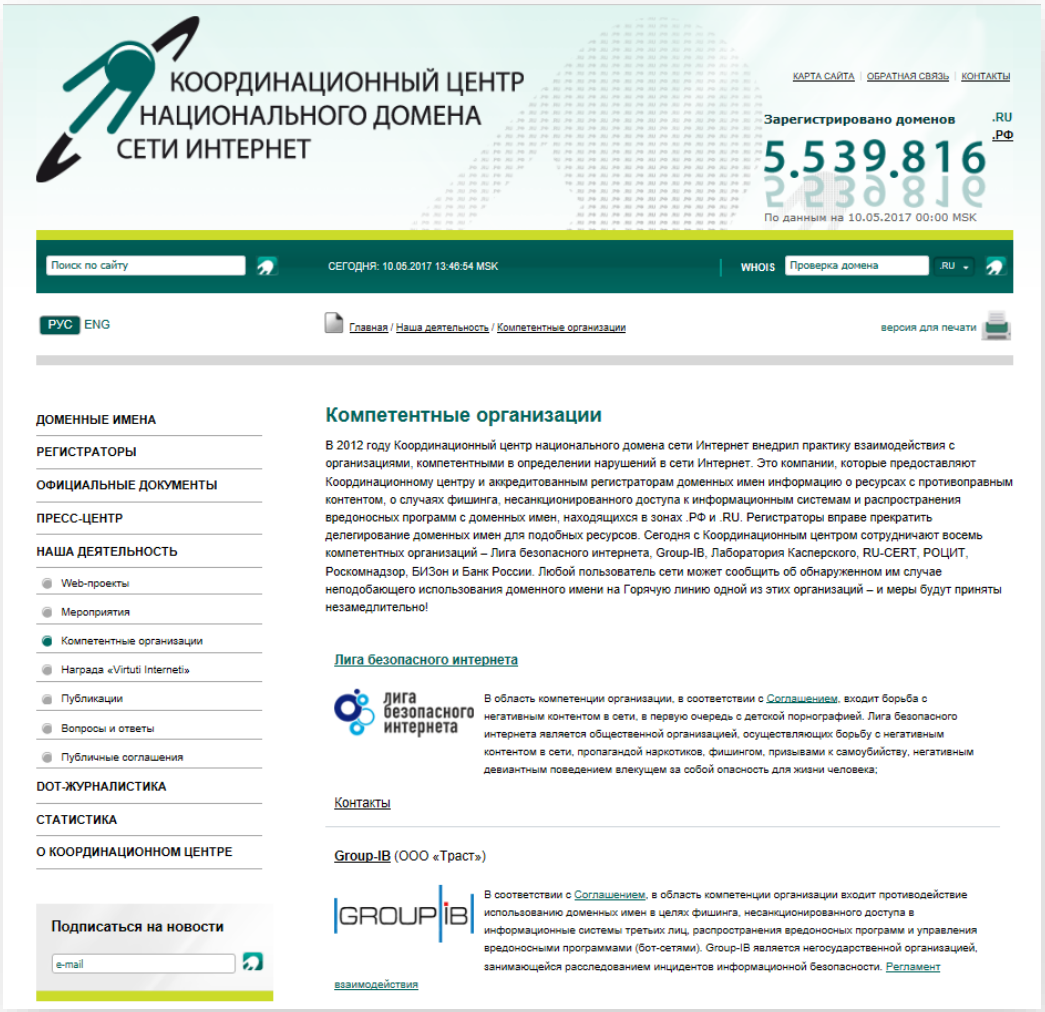
В социальных сетях создаются фейковые аккаунты, через которые от имени руководства ведомства распространяются ложные сведения

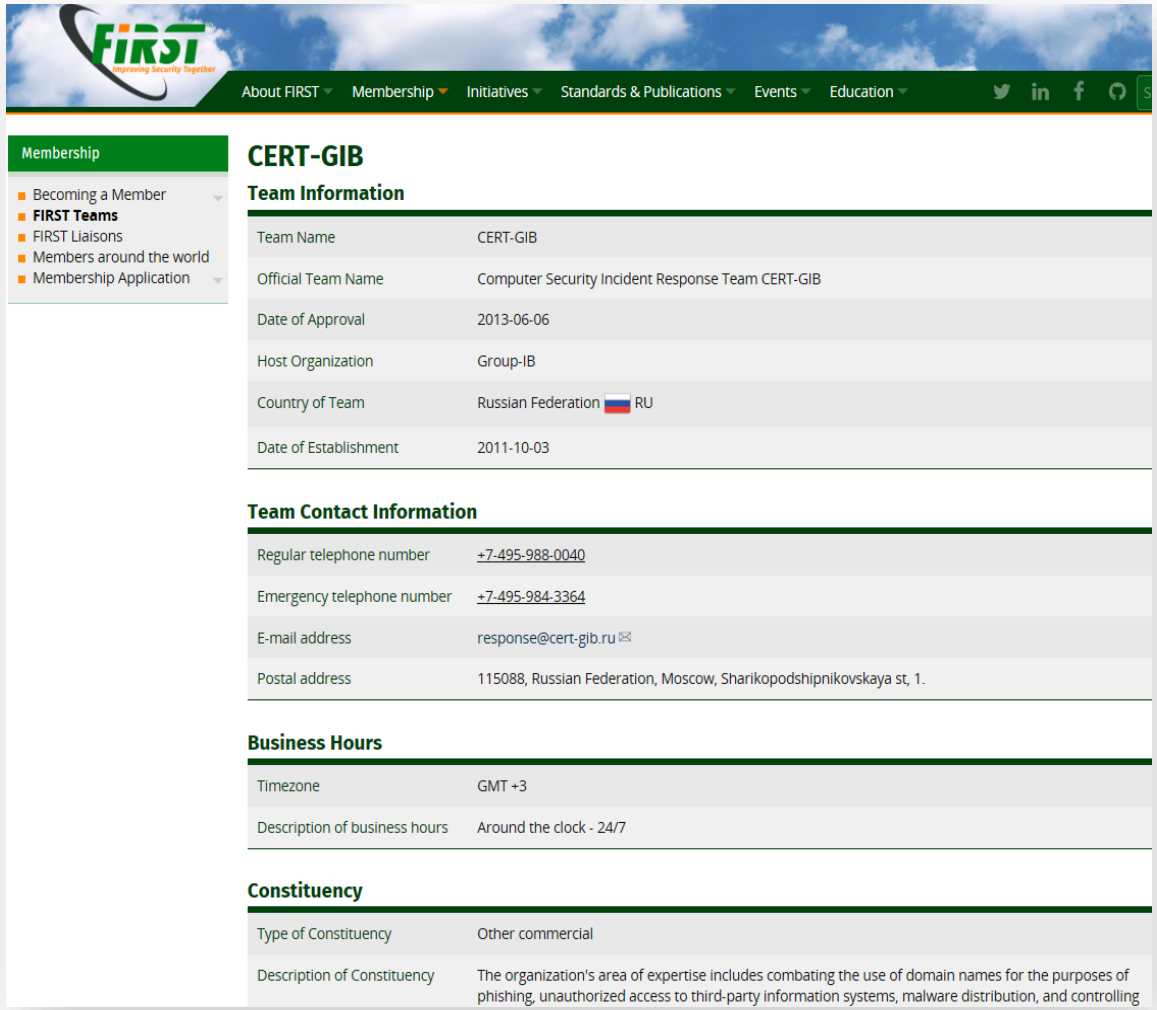
Долгосрочный репутационный ущерб

Утрата доверия к электронным сервисам Правительства

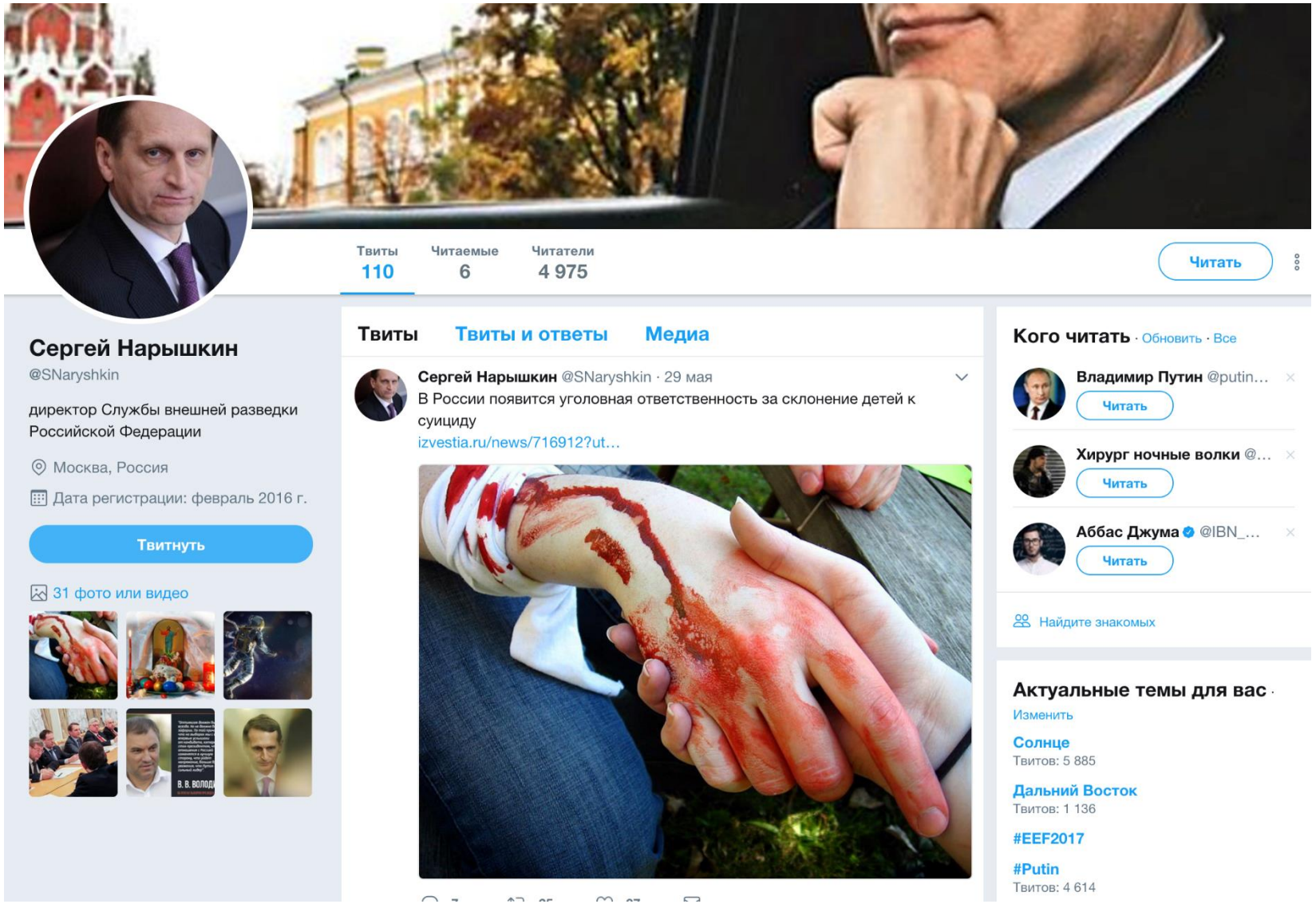
Издержки на урегулирование претензий жертв мошенничества

Компетенции GIB. Досудебная блокировка нарушений





Фейковые профили в социальных сетях



Взлом аккаунтов



11. Дмитрий Медведев, премьер-министр России
Аккаунт: @MedvedevRussia

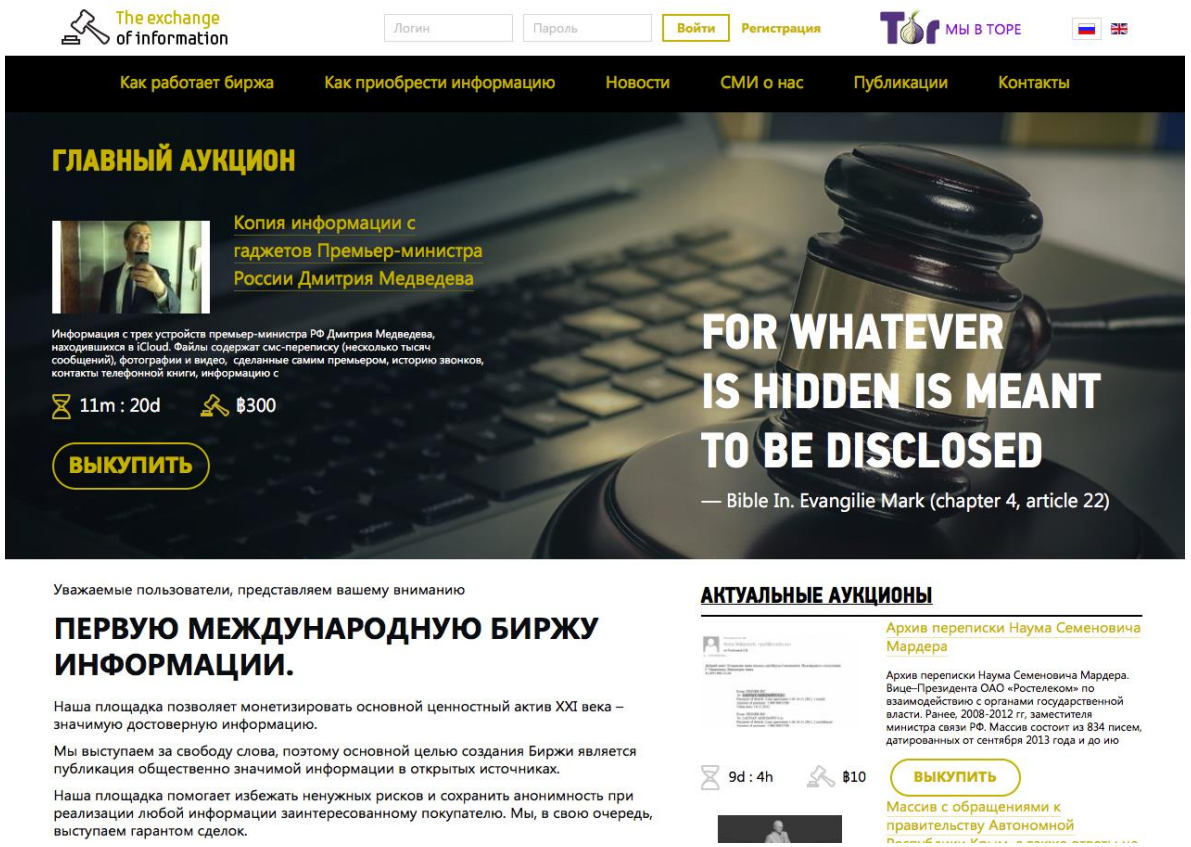
Количество подписчиков: Более 3, 7 миллионов

В Твиттере: с июня 2010 года

Главный популяризатор Twitter в России, который ввел моду на эту социальную сеть среди российских чиновников. Дмитрий Медведев завел микроблог в 2010 году во время посещения штаб-квартиры Twitter в Кремниевой долине. Тогда его аккаунт назывался KremlinRussia, а позже был переименован в @MedvedevRussia.

В прошлом году группа хакеров, получив доступ к копиям смартфонов российского премьера, взломала его аккаунт в Twitter и оставила там несколько твитов, например «Ухожу в отставку. Стыдно за действия правительства. Простите». Доступ к микроблогу оперативно был возвращен владельцу.

Взлом аккаунтов



Хакеры опубликовали электронные письма Дворковича

Вице-премьер обсуждал рабочие вопросы в личной почте на Gmail

Общество • 22 июля 2014

Хакеры сообщили о взломе почты и WhatsApp известного телеведущего Дмитрия Киселева

29.04.2016 | 17:59

Хакеры выложили в сеть переписку чиновника из Кремля Тимура Прокопенко

31 марта 2015 20:02 Политика » Главное политика



Группировка хакеров "Анонимный интернационал" выложила в сеть архив, содержащий около 40 тысяч смс-сообщений.

Они были скачаны, вероятно, с мобильного телефона Тимура Прокопенко, который с осени 2012 года по зиму 2014-го курировал в администрации президента России интернет.

Фальшивые e-mail рассылки

газета.ru

НОВОСТИ ПОЛИТИКА БИЗНЕС ОБЩЕСТВО АРМИЯ МНЕНИЯ КУЛЬТУРА НАУКА ТЕХНОЛОГИ



Хакеры выключают Америку

Американские объекты энергетической инфраструктуры подверглись хакерской атаке, целью которой был поиск уязвимостей системы. Спецслужбы полагают, что... →

За неделю до этого специалисты по компьютерной безопасности обнаружили фишинговую атаку, замаскированную под уведомления о штрафах с портала госуслуг.

Как рассказали в компании Group-IB, специализирующейся на предотвращении компьютерных преступлений, хакеры рассылают письма-уведомления якобы о наличии штрафа ГИБДД. К письму прикреплено фото автомобиля, совершающего нарушение. При этом в шапке письма находится логотип Электронного правительства.

Кроме того, отмечалось, что письмо содержит отметку о проверке файлов на вирусы и об их отсутствии. Мошенники делали акцент на том, что получить скидку в 50% можно, только оплатив штраф в течение короткого времени.

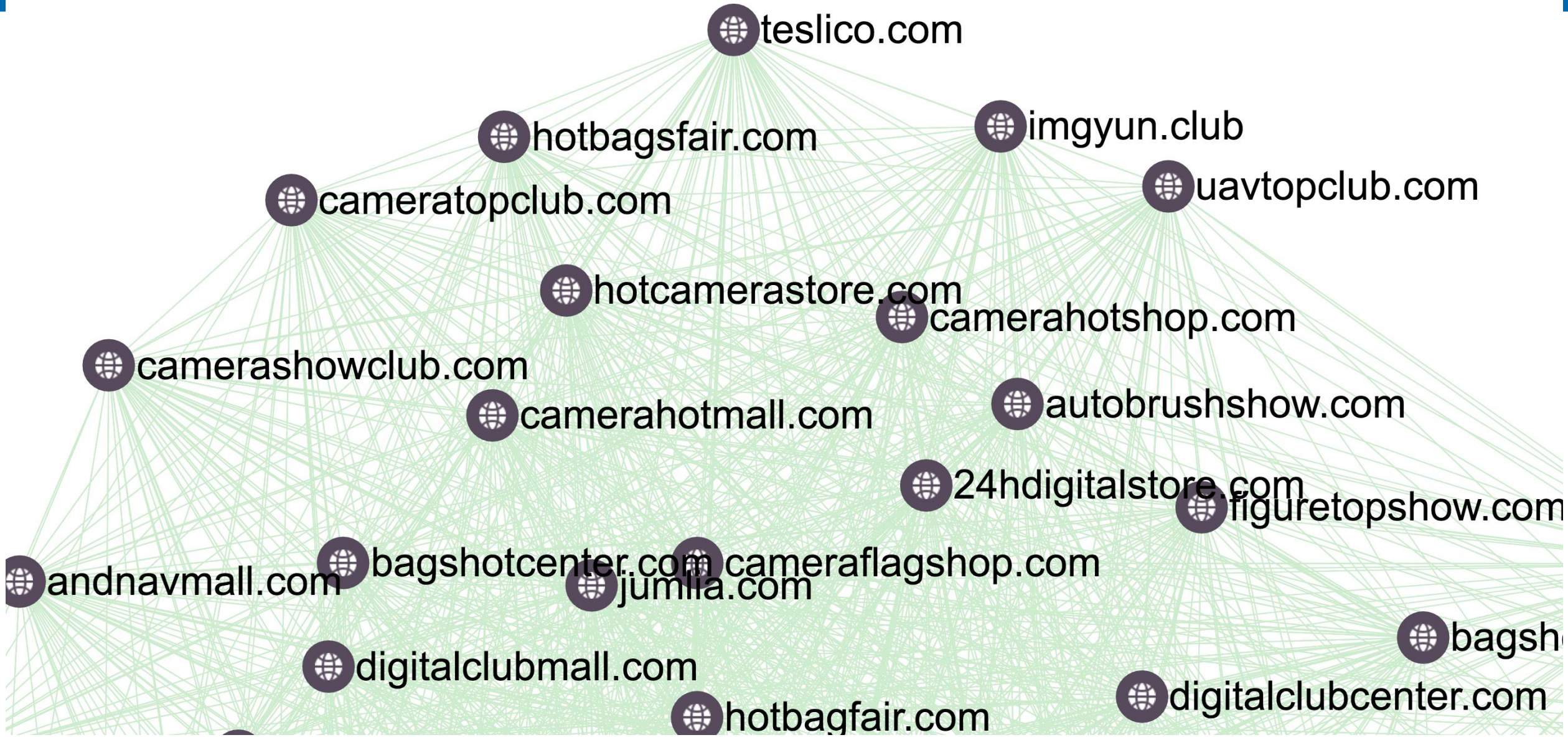
Анализ инфраструктуры злоумышленника



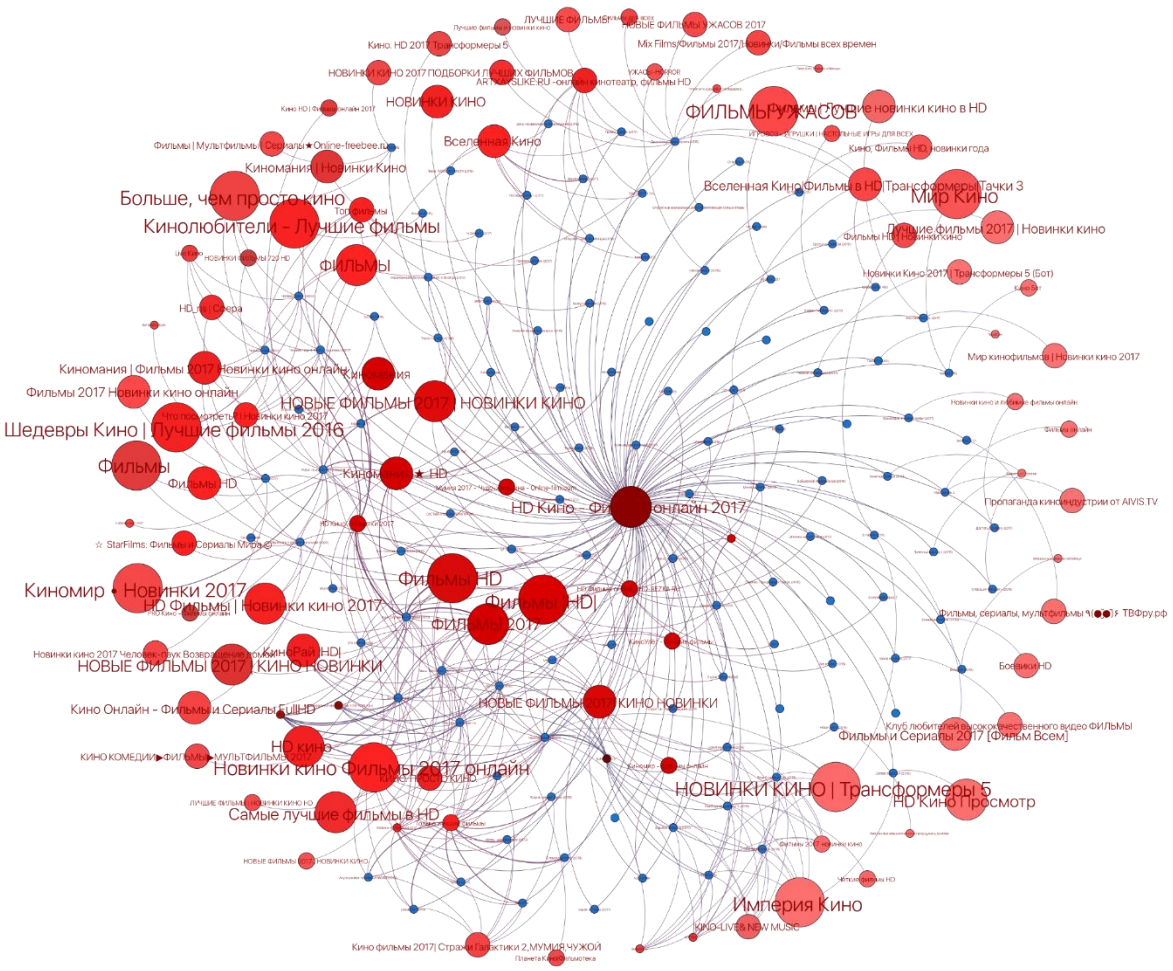
Domains 12 | IP addresses 8 | SSH fingerprints 0 | SSL-certificates 1 | Files 0 | Email 3 | Phone 4 | Neighbours | Communities

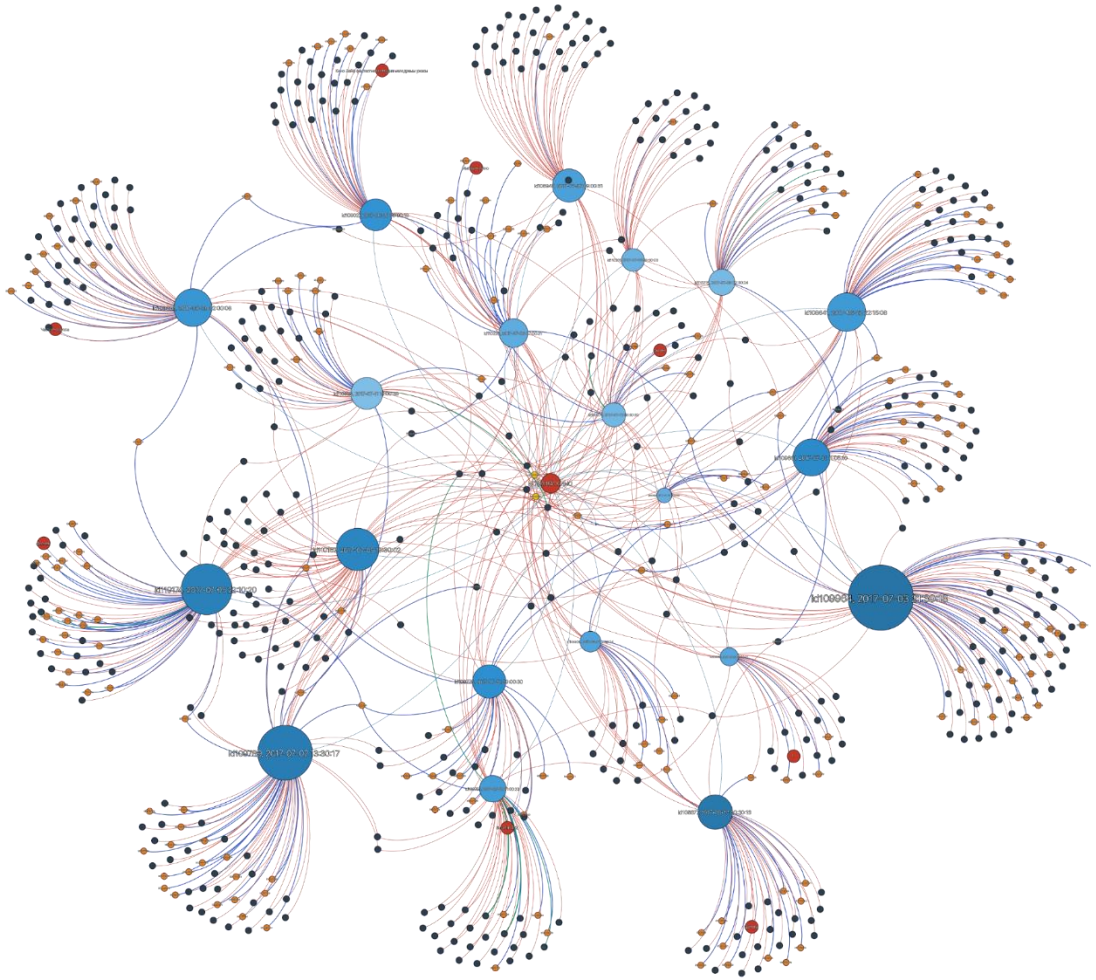
Domain name	Registrar	Reg date	Exp date	Email	Phone	Organization	Name	IP-address
yastreb.net	REGISTRAR OF DO...	2009-02-17	2016-02-17	paytraf@gmail.com	+74955123456	Private Person	Valery Viktorov	62.233.65.46
rus.porn	Tucows Domains Inc.	2016-01-19	2017-01-19	paytraf@gmail.com	+7.4955123456	Private Person	Valery Garifzyanov	93.158.134.250
fizruk2sezon.org	PDR Ltd. d/b/a Publi...	2014-11-29	2016-11-29	paytraf@gmail.com	+972.972547747468	N/A	Valery Garifzyanov	91.201.202.56

Пример инфраструктуры злоумышленника



Аналитика и аффилированность в социальных сетях





Защита от мошеннических действий, направленных на органы государственной власти

Мониторинг и предотвращение экономических преступлений и мошенничества с использованием бренда

Круглосуточный мониторинг более 4 000 000 ресурсов:

- Даркнет
- Сайты
- Социальные сети
- Мессенджеры
- Магазины мобильных приложений
- Рекламные сети (Яндекс.Директ, Google AdWords)
- E-mail рассылки
- Спам
- СМС рассылки



Сбор цифровых доказательств



Идентификация владельца площадки



Блокировка опасных сайтов в течение 24 часов



Возможность реагирования за пределами Рунета



Предотвращение рецидивов



Круглосуточный мониторинг

Угрозы и решения

Угроза: компрометация аккаунтов и устройств госслужащих

В 2016 году объем хищений с помощью троянов мобильных устройств в России впервые превысил объем хищений с помощью троянов для ПК.

Только за январь 2017 система киберразведки Group-IB обнаружила заражения более 125 000 пользователей мобильных устройств.

200 пользователей были заражены трояном Marcher, совмещающим функционал для хищений с широкими возможностями шпионажа за владельцем.



Решение: кибербразведка

Сведения о скомпрометированных аккаунтах и детальный контекст угрозы: где, как, с помощью каких программ атаковали жертву, что известно о преступниках

КОРПОРАТИВНЫЕ АККАУНТЫ

Учетные записи, связанные с корпоративными доменами и диапазонами IP: e-mail аккаунты, доступы к intranet-ресурсам и т.д.

Пресекайте шпионаж, утечки и другие последствия взлома

Идентифицируйте ресурсы компании, к которым подключались с использованием скомпрометированных записей

Устаналивайте взаимосвязи с другими инцидентами

МОБИЛЬНЫЕ ТЕЛЕФОНЫ

IMEI зараженных телефонов клиентов и сотрудников

Оповещайте клиентов о заражении устройств

Проверяйте наличие других зараженных телефонов, связывающихся с этим же центром управления бот-сетью

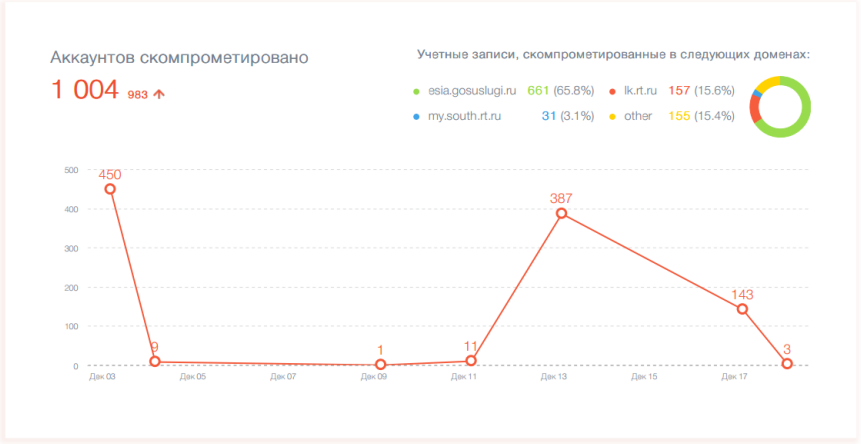
Интегрируйте данные в Mobile Device Management системы

Угрозы и защита

Угроза: хищение персональных данных и мошенничество на гос порталах

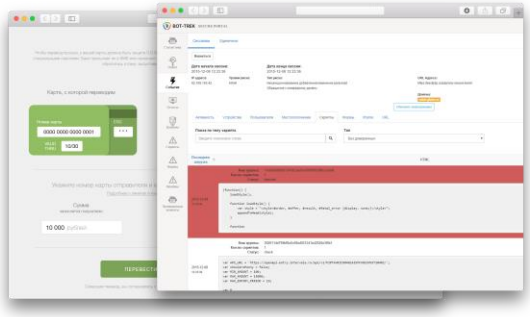
Пример того как система киберразведки Group-IB, мониторит украденные пароли от аккаунтов, адресов электронной почты, облачных сервисов на доменах, относящихся к компании.

В частности, преступники получили доступ к индентификаторам более 650 пользователей портала «Госуслуги».



Защита гос порталов и облачных сервисов

Незаметно загружаясь вместе со страницами портала, модуль мгновенно собирает информацию, которая помогает выявить мошенническую активность, и уведомляет администраторов об угрозе.



Работа модуля не сказывается на скорости загрузки страниц

Secure Portal выявляет:

- несанкционированный доступ к личным кабинетам и персональным данным
- сбор данных о платежных картах и использованные ворованных карт
- использование ботов (для подбора паролей, накрутки голосов)
- новые методы мошенничеств на стороне пользователей

ТЕКУЩИЕ КЛИЕНТЫ

СБЕРБАНК

АЭРОФЛОТ Российские авиалинии

М.видео

Как узнать об актуальных угрозах

Каждый год мы публикуем отчет о тенденциях высокотехнологичных преступлений и прогнозы их развития - прогнозы, которые сбываются

2014



2015



2016



2017 новый!



Скачать: www.group-ib.ru/2017-report.html

Предотвращаем и расследуем киберпреступления с 2003 года

www.group-ib.ru

blog.group-ib.ru

facebook.com/group-ib

info@group-ib.ru

+7 495 984 33 64

twitter.com/groupib



Илья Сачков, генеральный директор и основатель Group-IB

www.group-ib.ru

facebook.com/ilya.sachkov
linkedin.com/in/ilyasachkov