-RUNET——ID-

eTicket

Masalovich Andrei

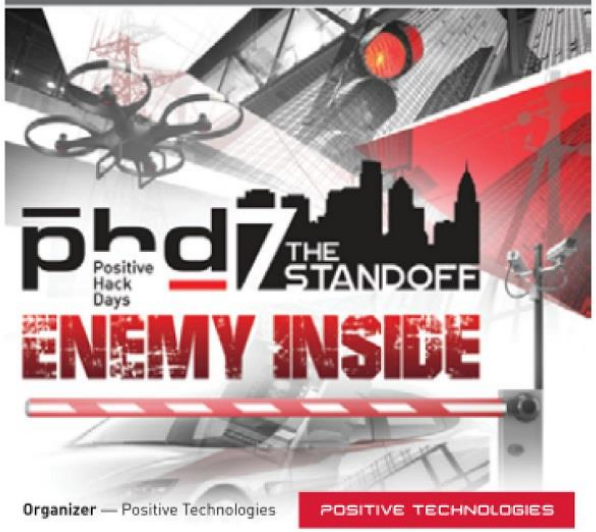
СПИКЕР

WTC MOSCOW

757308

To pass to the event You must present a ticket

-RUNET——ID-



Ты, а не тебя

Армии умных ботов в руках хакера

The Forum is organized by Positive Technologies
phone: +7 495 744 01 44;
e-mail: phd@ptsecurity.com;

#phdaysVII
#phdays7

f@phdays

-RUNET——ID-

Будни Интернета: война ботов

- В докладе на реальных примерах рассматриваются технологии «умных ботов»: армия ботов позволяет за полчаса подобрать пароли от миллиона почтовых ящиков, взломать код верификации (cvv) кредитки, перехватить управление десятками аккаунтов в Facebook и т.д.
- Высокоорганизованные боты «информационного спецназа» обеспечивают практически мгновенную доставку ударного контента в места скопления целевой аудитории.
- «Умные боты» используются и на стороне добра — для борьбы с пиратами, мошенниками, вымогателями и экстремистами.

Stand or Fall.

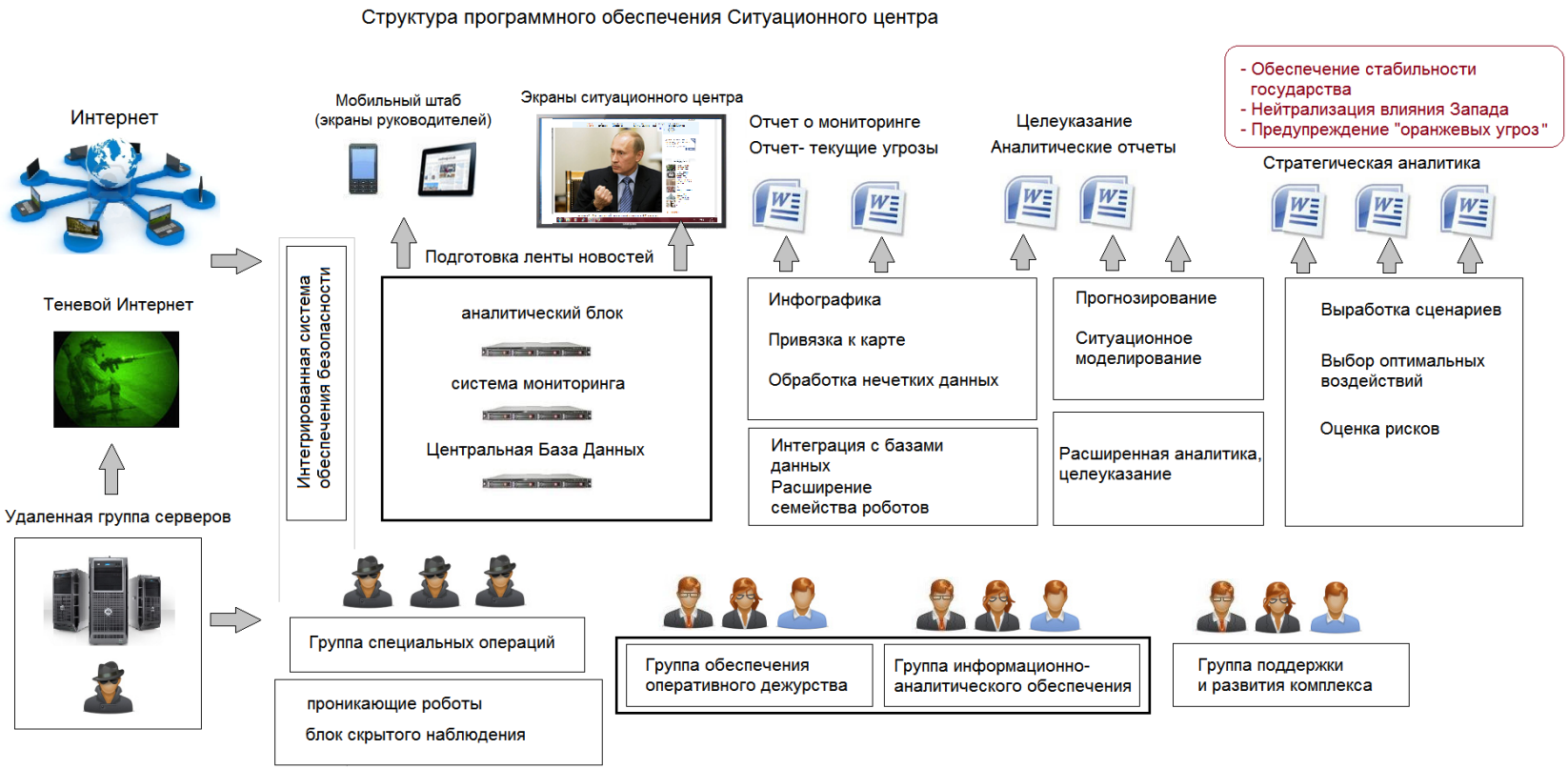
An army of intelligent bots controlled by hackers

These days, the Web Standoff is not just a warfare between humans and bots, we are talking about a botnet programmed to act in an intelligent, user-like manner, an army with a proper coordination. DDoS botnets have evolved from a basic tool to a powerful weapon of information confrontation in the hands of hackers, intruders, and intelligence services.

The speaker will share some real-life examples: from massive password hacking to influencing electoral outcomes.

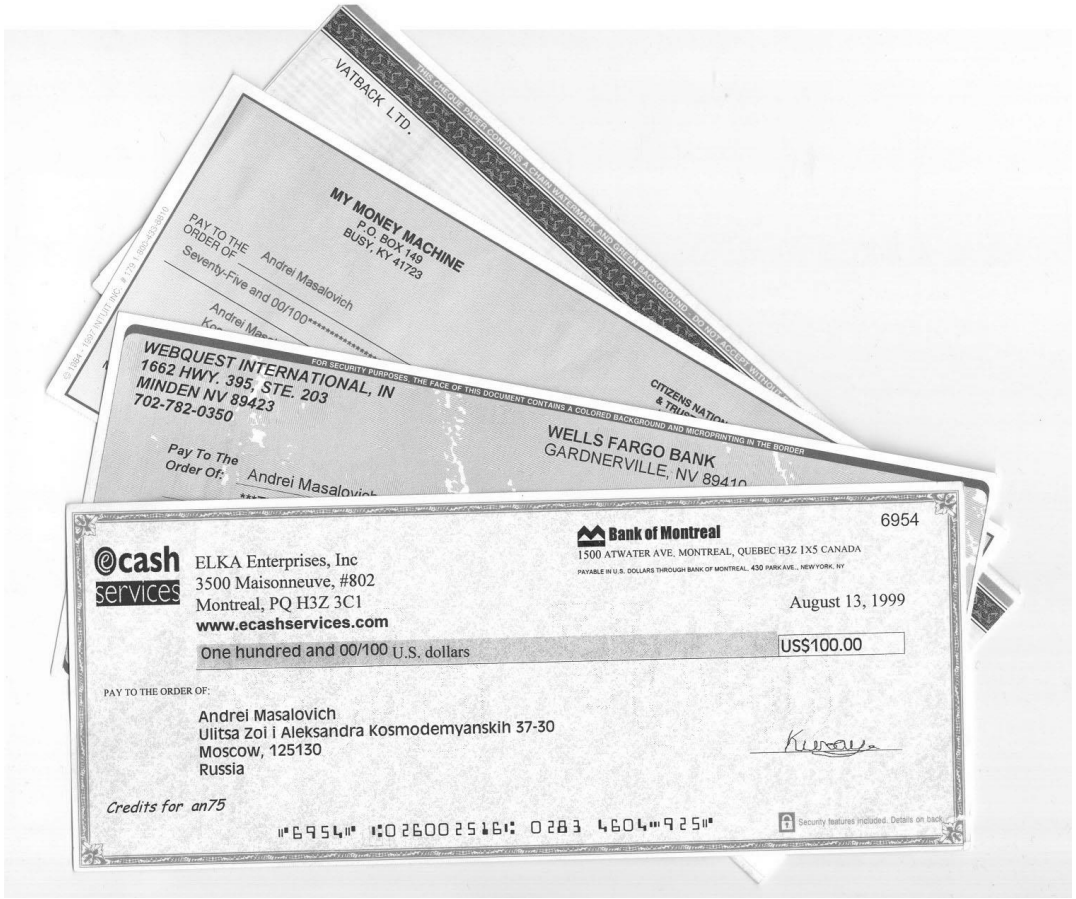
AVALANCHE

Технологическая платформа информационного противоборства



Новый взгляд на взлом

The Hacker


VATBACK LTD.
MY MONEY MACHINE
P.O. BOX 149
BUSY, KY 41723
PAY TO THE ORDER OF
Andrei Masalovich
Seventy-Five and 00/100
WEBQUEST INTERNATIONAL, IN
1662 HWY. 395, STE. 203
MINDEN NV 89423
702-782-0350
Pay To The Order Of:
Andrei Masalovich
WELLS FARGO BANK
GARDNERVILLE, NV 89410
6954
ecash services
ELKA Enterprises, Inc
3500 Maisonneuve, #802
Montreal, PQ H3Z 3C1
www.ecashservices.com
Bank of Montreal
1500 ATWATER AVE, MONTREAL, QUEBEC H3Z 1X5 CANADA
August 13, 1999
One hundred and 00/100 U.S. dollars
US$100.00
PAY TO THE ORDER OF:
Andrei Masalovich
Ulitsa Zoi i Aleksandra Kosmodemyanskih 37-30
Moscow, 125130
Russia
Credits for an75

Definition - What does *Internet Bot* mean?

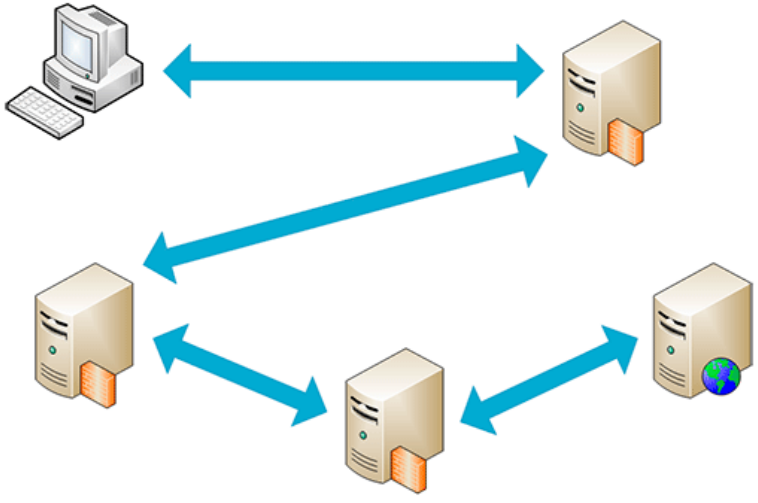
- An Internet Bot, also known as web robot, WWW robot or simply bot, is a software application that runs automated tasks (scripts) over the Internet.
- Typically, bots perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone.
- The largest use of bots is in web spidering (web crawlers)
- More than half of all web traffic is made up of bots.

«Smart Bot» avoids Captha

Обходим капчу: два бота и один хакер

1. Бот получает капчу
   и передает ее
   на подконтрольный форум.
2. Посетитель форума получает
   сообщение «Подтвердите,
   что вы не робот»
   – и заполняет капчу

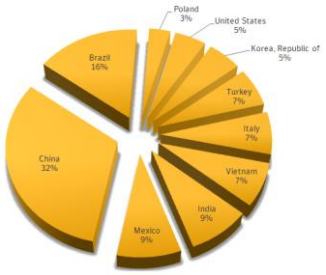
Guccifer 2.0 Hacked Clinton Foundation. How?



```
import todos from './ui/reducer';
import ui from './users/reducer';
import users from './auth/actions';
import { LOGOUT } from './app/actions';
import { UPDATE_APP_STATE_FROM_STORAGE_SUCCESS } from 'redux';
import { combineReducers } from 'redux';
import { fieldsReducer as fields } from './lib/redux-fields';
import { firebaseReducer as firebase } from './lib/redux-firebase';
import{ routerReducer as routing } from 'react-router-redux';

//Guccifer 2.0 was here//

// Reset app state on logout, stackoverflow.com/q/35622588/233902.
const resetOnLogout = (reducer, initialState) => (state, action) =>
  if (action.type === LOGOUT) {
    // Delete whole app state except some fixtures and routing state.
    state = {
      device: initialState.device,
      intl: initialState.intl,
      routing: state.routing // Note routing state has to be reused.
    };
```

Linux.Wifatch – добрый ботнет

- Обнаружен компанией Symantec, ноябрь 2014
- Заражает сетевые устройства через уязвимость в службе Telnet
- Объединяет зараженные устройства в сеть peer-to-peer
- Написан на Perl, содержит интерпретаторы для каждой архитектуры
- Использует сжатие кода, но не обфускацию
- Не проявляет деструктивной активности
- Пытается найти и завершить работу известных вредоносных программ
- Настраивает перезагрузку для чистки памяти
- Убивает уязвимый демон Telnet
- Просит администратора отключить уязвимую службу, сменить пароли или обновить прошивку



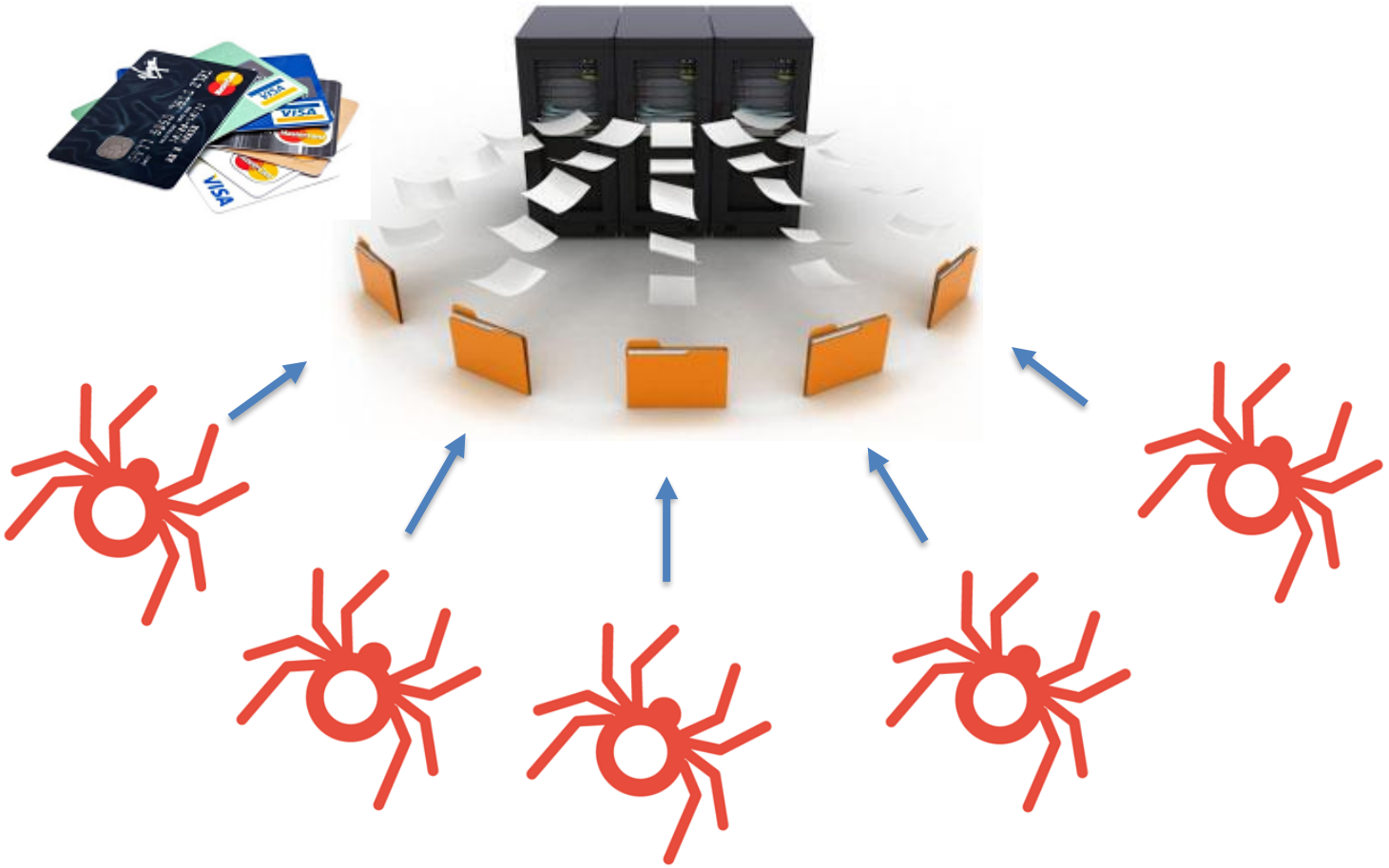

```
$ telnet
Trying                ..
Connected to
Escape character is '^]'.

REINCARNA

Telnet has been closed to avoid further infection of this device. Please
disable telnet, change telnet passwords, and/or update the firmware.

Connection closed by foreign host.
$
```

Does The Online Card Payment Landscape Unwittingly Facilitate Fraud?

- 389 магазинов из ТОП-400 не препятствовали анализу защищенности
- 291 магазин проверяет всего три поля карты (номер карты, срок действия и CVV)
- 26 магазинов проверяют всего два поля карты
- Только 25 магазинов делают дополнительные проверки
- Только 47 используют технологию защиты 3-D Secure
- Бот на Selenium подбирает CVV для VISA за 6 секунд

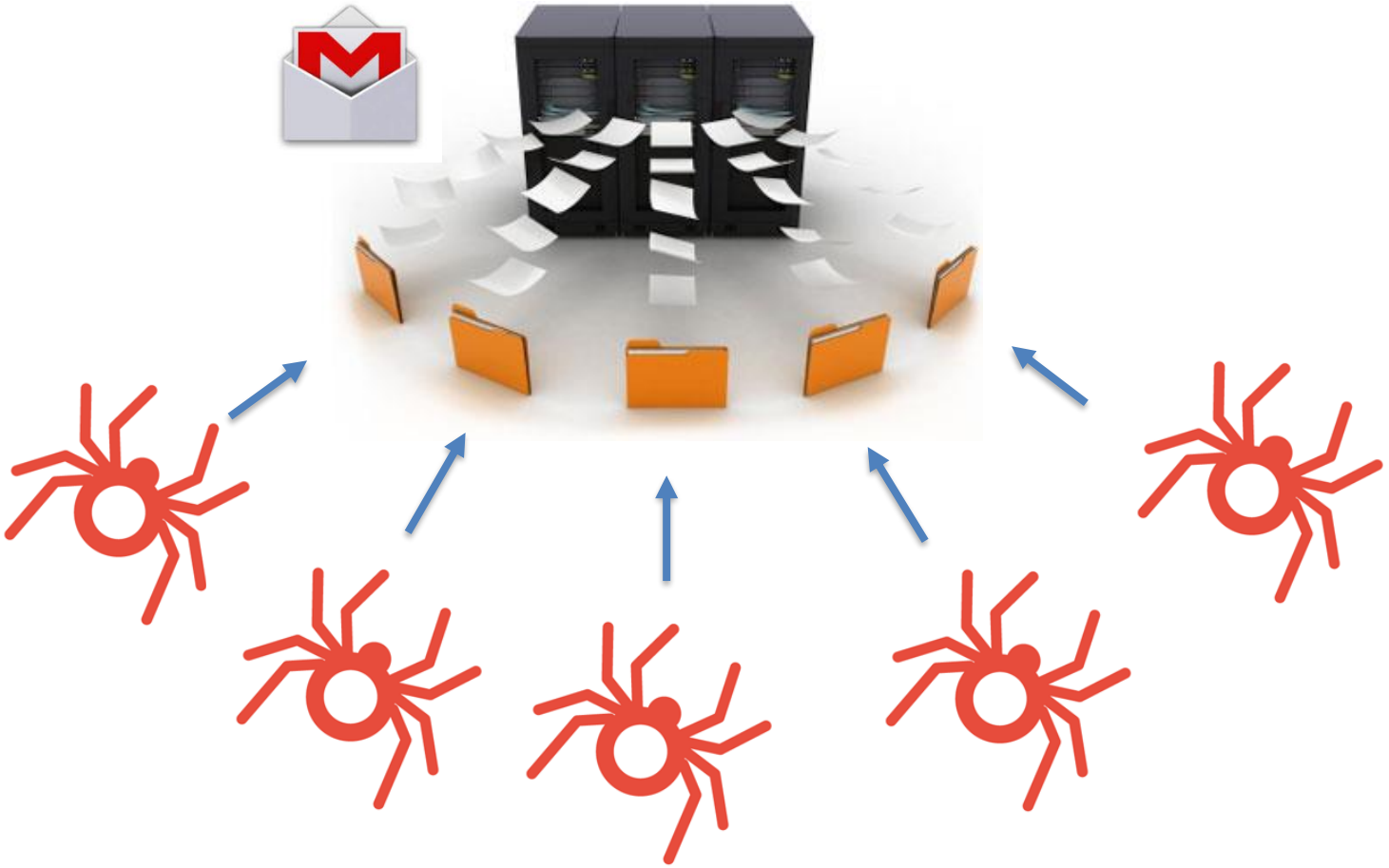
Источник: http://eprint.ncl.ac.uk/pub_details2.aspx?pub_id=230123%20

“CVV” Brut force:
smart bots crack your credit card



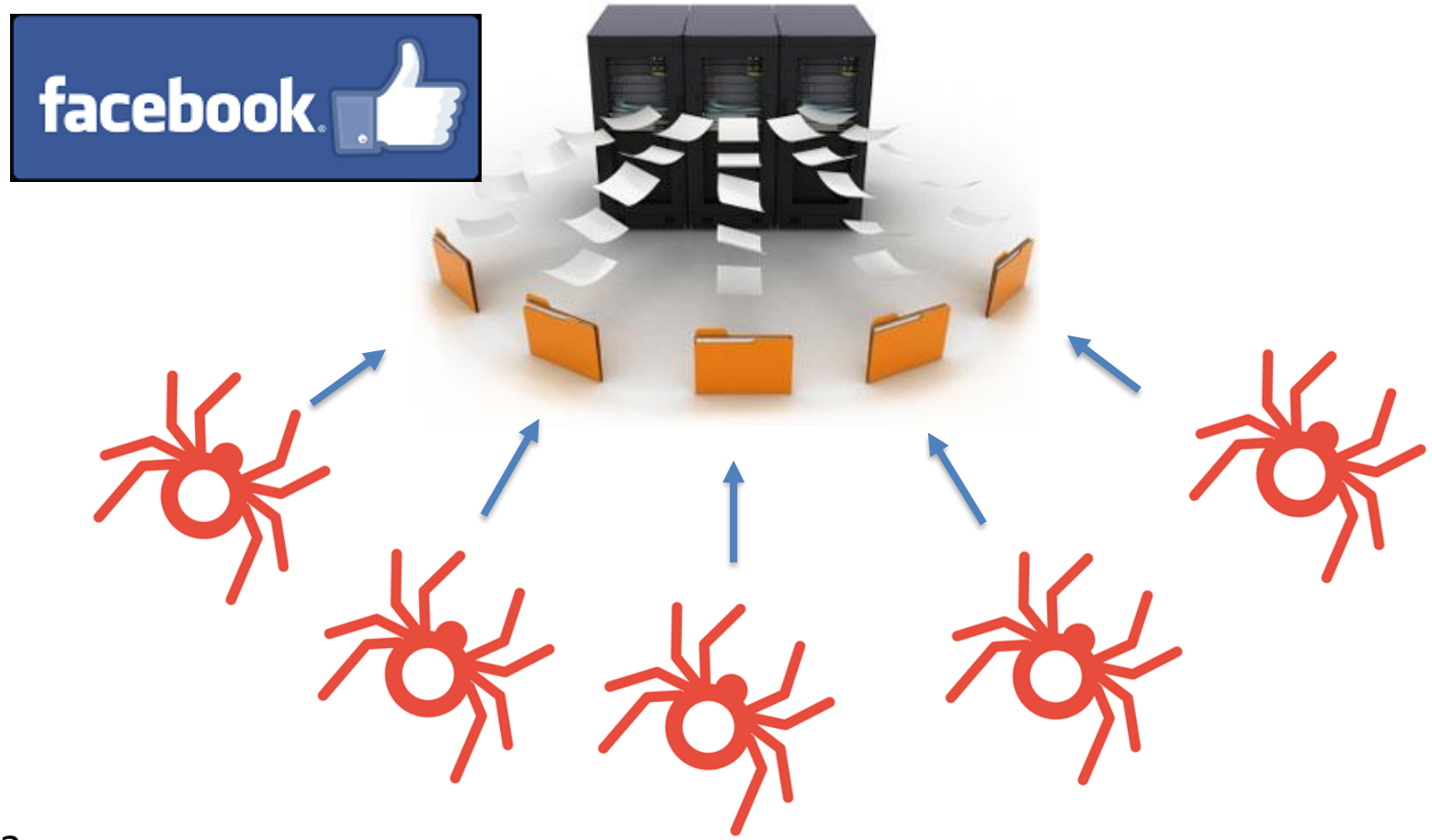
Multi-Login Brutforce: smart bots attack mail server

«Горизонтальный брутфорс»



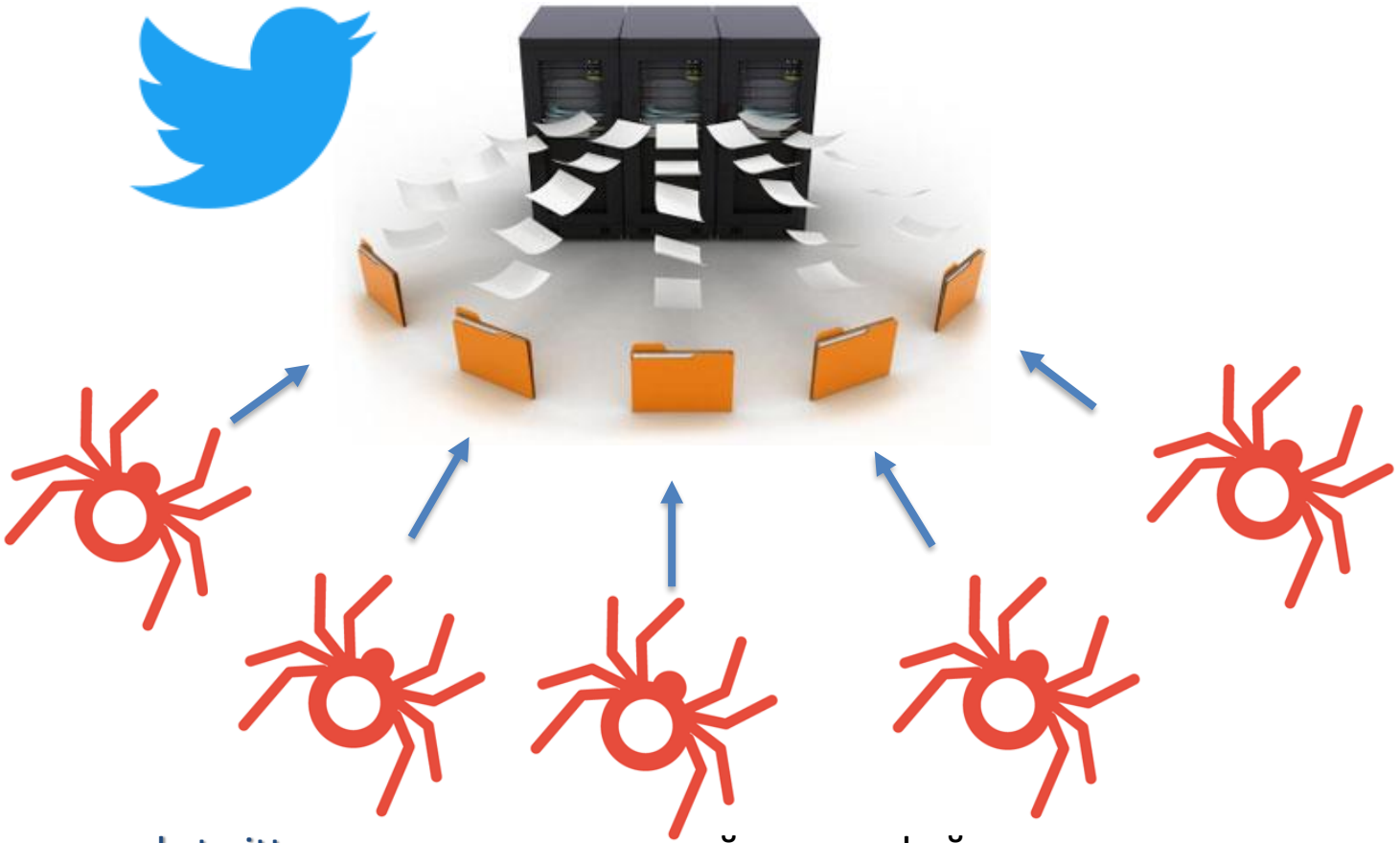
- Подбор паролей к заданному логину будет пресечен сразу
- Попытки зайти с одним паролем с тысяч логинов сервер не блокирует

“Forget Password” Brut force: smart bots attack Facebook server



1. Запрашиваем восстановление своего пароля – получаем код подтверждения
2. Запрашиваем восстановление пароля от имени миллиона пользователей, подставляем свой код подтверждения. Примерно 20 аккаунтов теперь наши.

How to crack Twitter

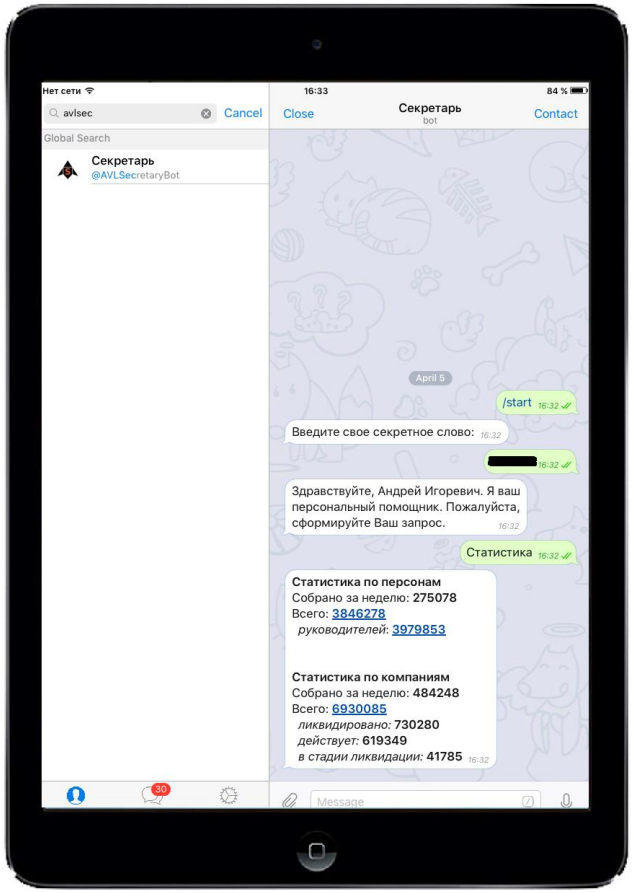


1. Заходим в ads.twitter.com, загружаем свой медиа-файл
2. Делимся этим файлом с аккаунтом жертвы
3. Перехватываем запрос публикации твита и подменяем в POST owner_id и user_id на id twitter аккаунта жертвы. Твит будет опубликован от его имени.

Источник: https://habrahabr.ru/company/dsec/blog/327904/

Новый взгляд на поисковые роботы и сканеры

Проект «Ясень» – поисковая система в невидимом интернете (Deep Web)



AVALANCHE

SQL-injection

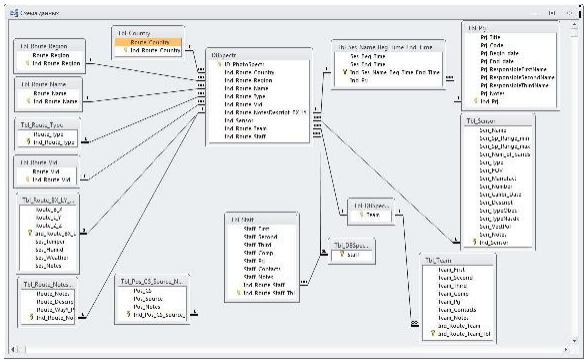
Взлом SQL-базы: сканер-хакер-бот

Шаг 1:

Сканер показывает уязвимость

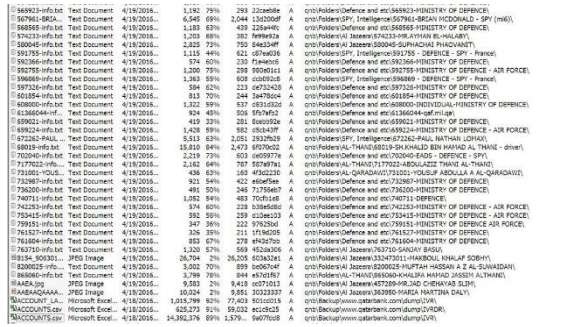
Шаг 2:

Хакер добывает схему данных



Шаг 3:

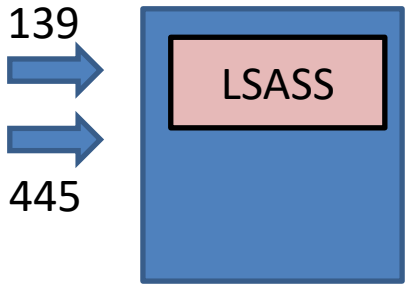
Бот атакует



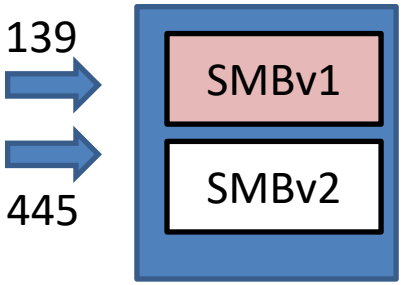
WannaCry, prehistoria

2004

Март-LSASS		Май-SASSER



2006



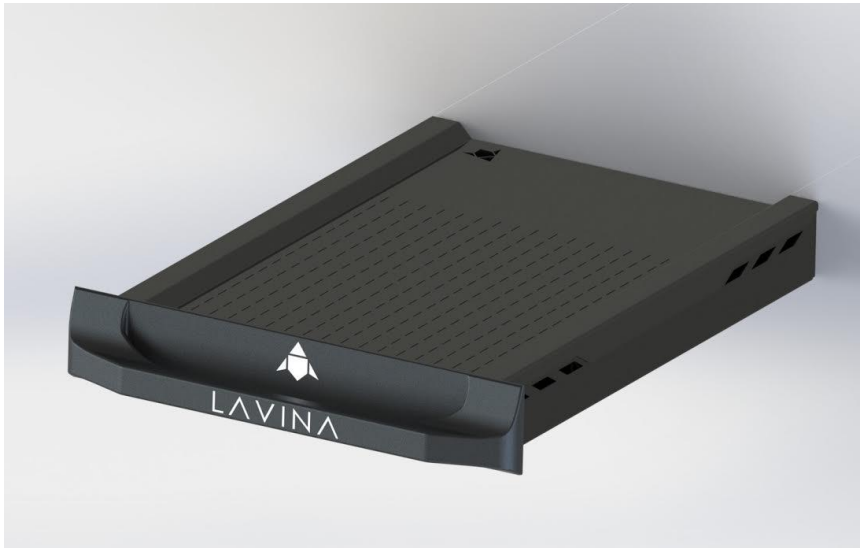
2017

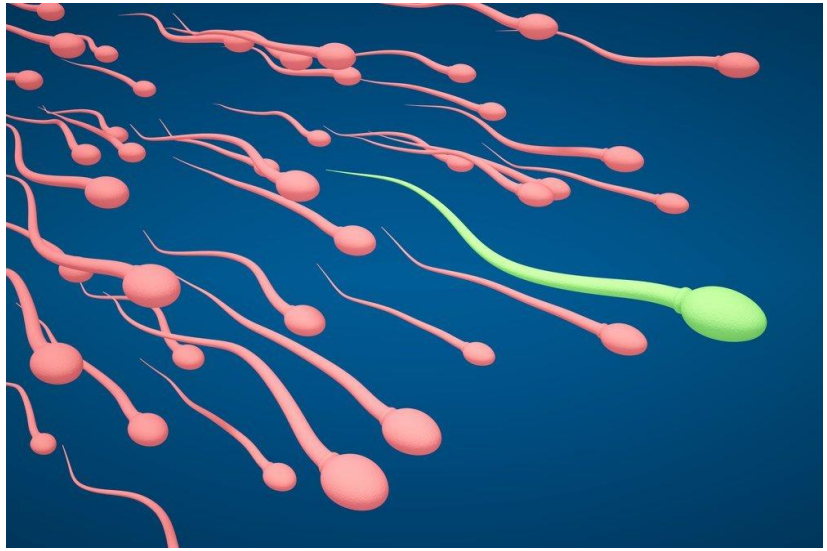
Март-MS017-10	WikiLeaks	Май-WannaCry

Внешнее сканирование – вакцина от вирусов

Уроки WannaCry:

- Изучен один ZeroDay из 120 (Ethernal Blue)
- Изучен один эксплоит (DoublePulsar) из ???
- Обнаружен один вредонос (WannaCry) из ???
- Ряд ведомств не пострадал. Случайность?





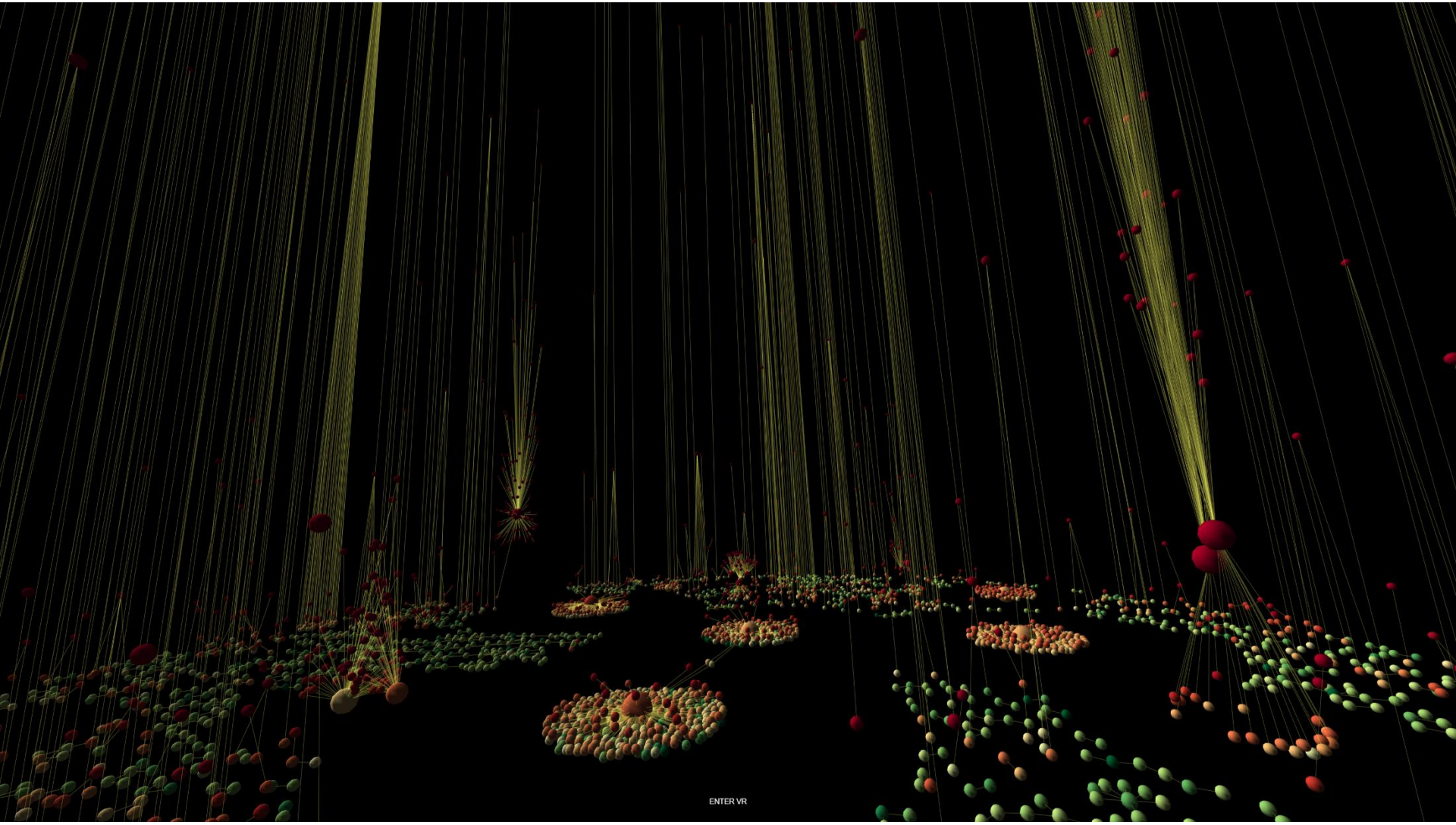
ЛАВИНА Сканер –активная защита нового поколения

Новый взгляд на противоборство

Step to the Web

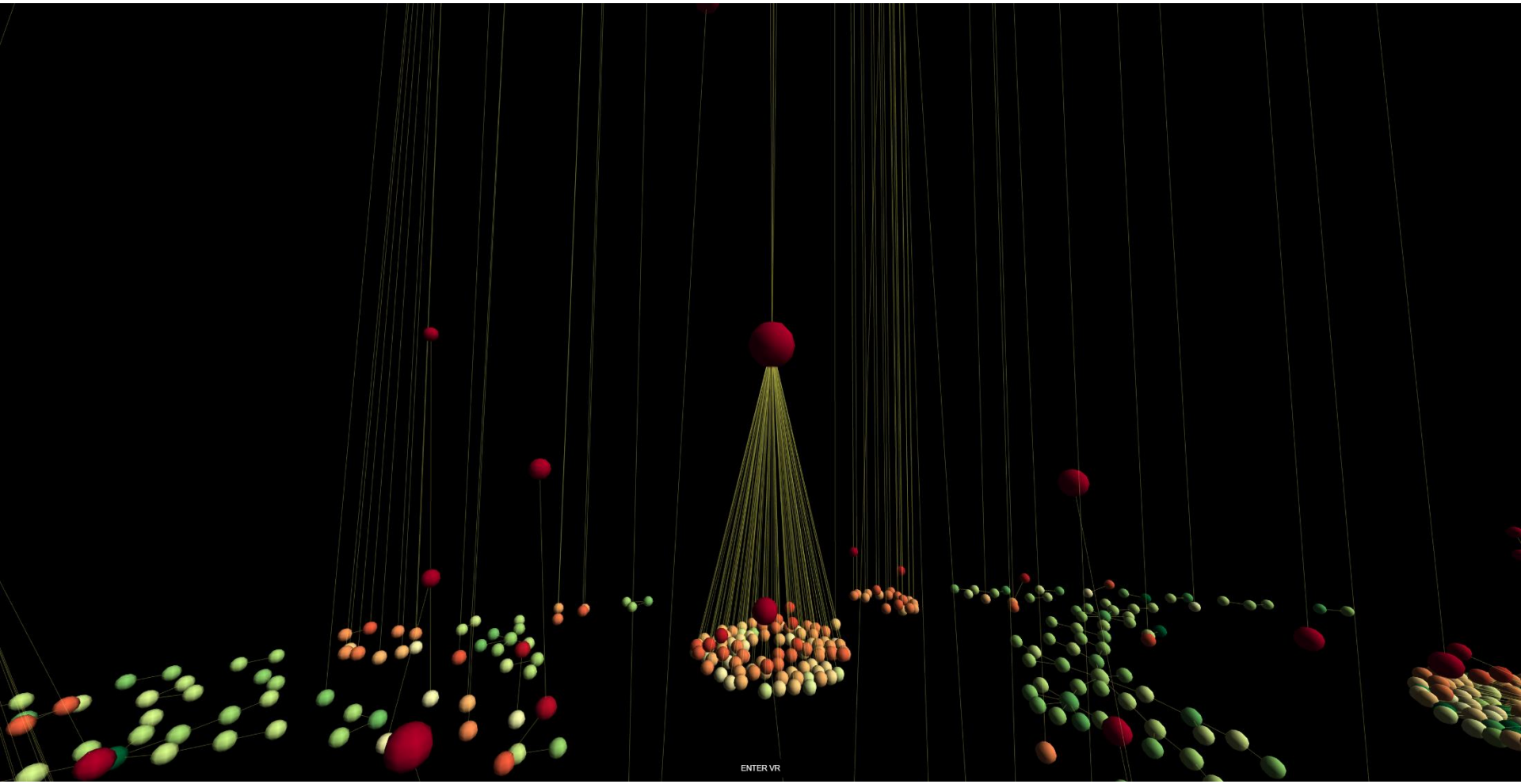
AVALANCHE

One minute inside Twitter



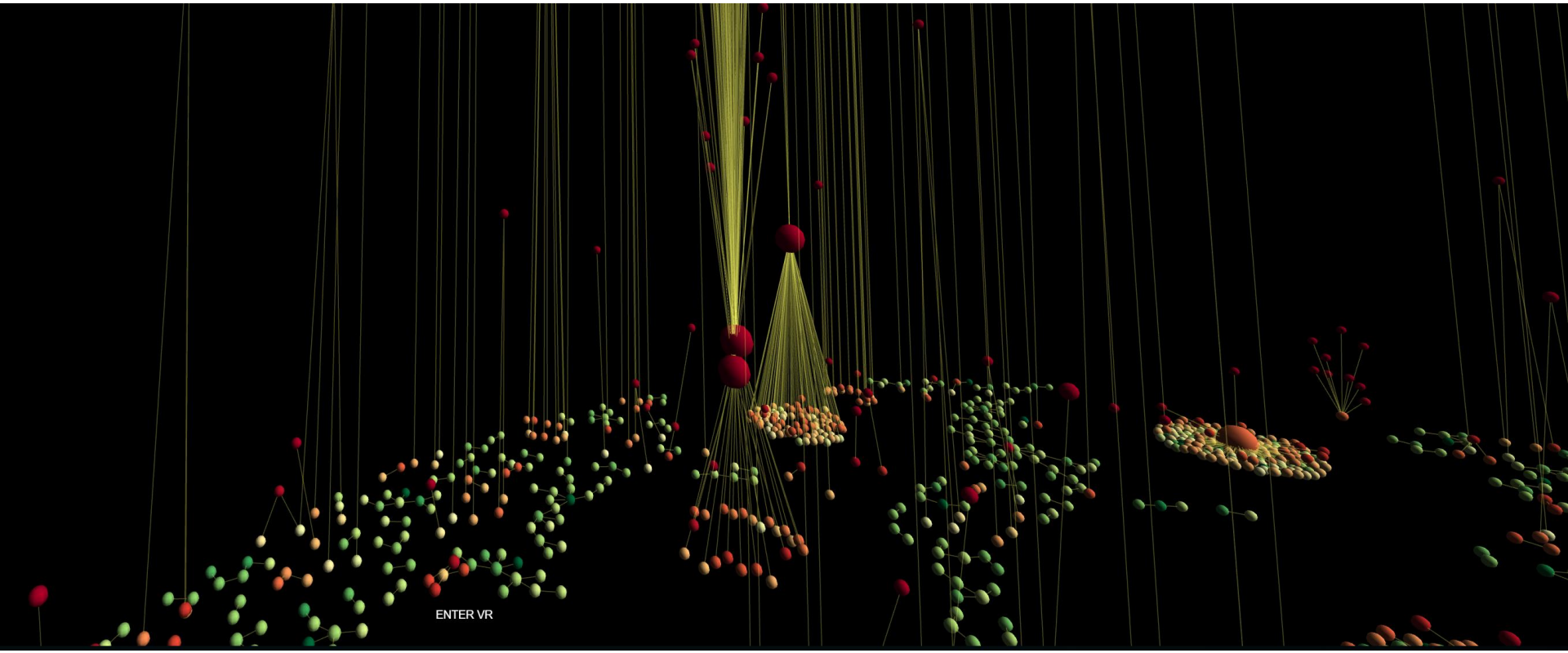
AVALANCHE

The Leader



AVALANCHE

Real People vs Botnets



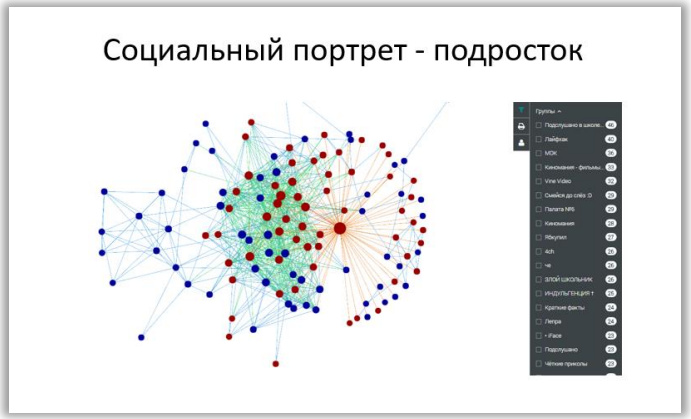
AVALANCHE

Behind Trump's victory: Russian Hackers or Russian Technologies?

Step 1: Psyhometrics

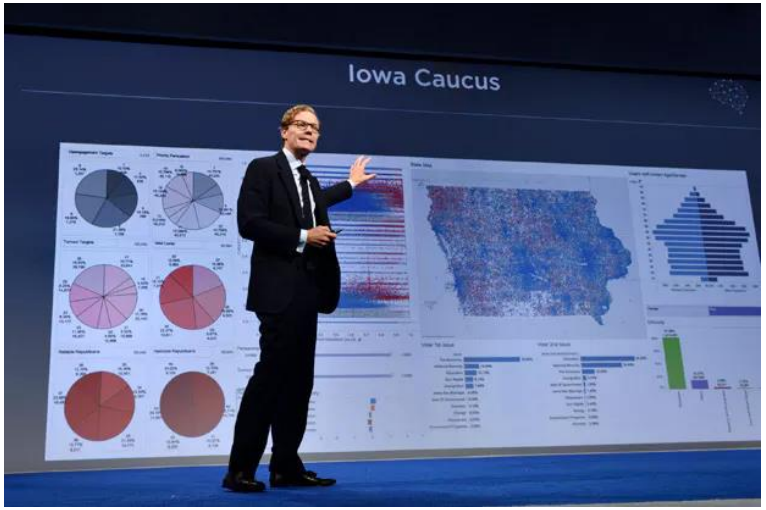
Psychometrics, a data-driven sub-branch of psychology

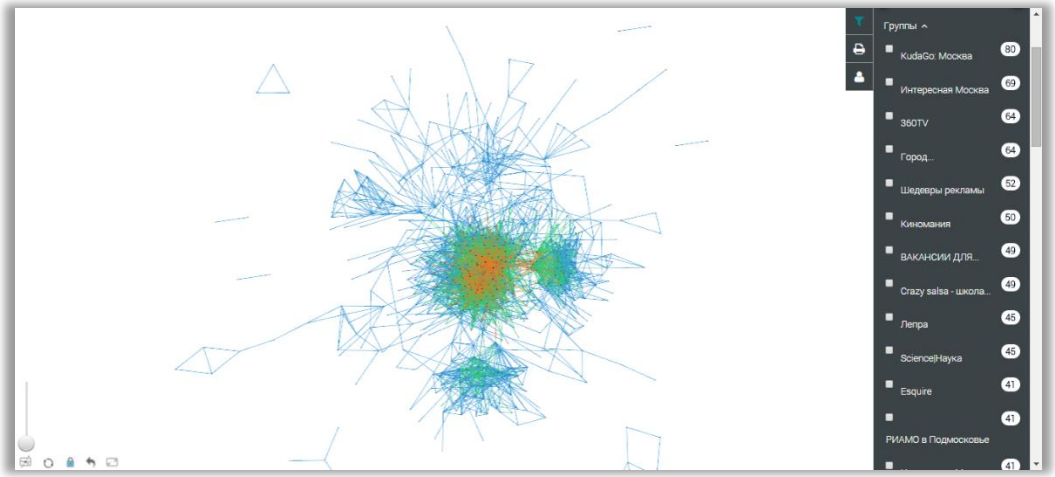
Анализа 68 лайков в Facebook достаточно, чтобы определить цвет кожи испытуемого (с 95% вероятностью), его гомосексуальность (88% вероятности) и приверженность Демократической или Республиканской партии



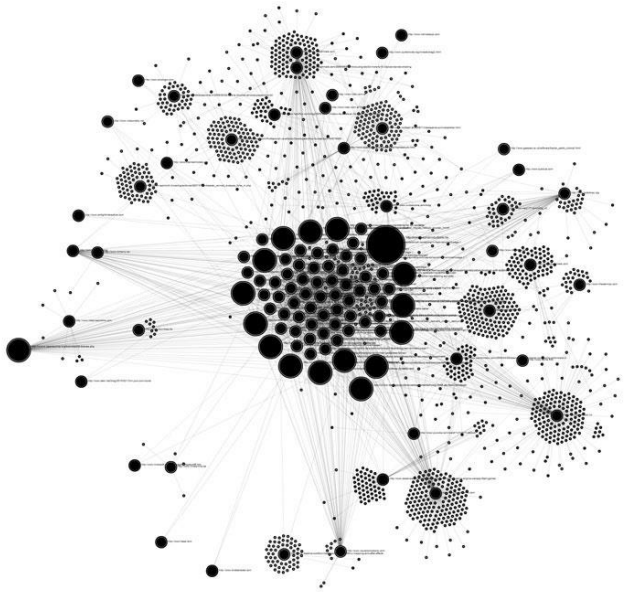
Step 2: Better audience targeting

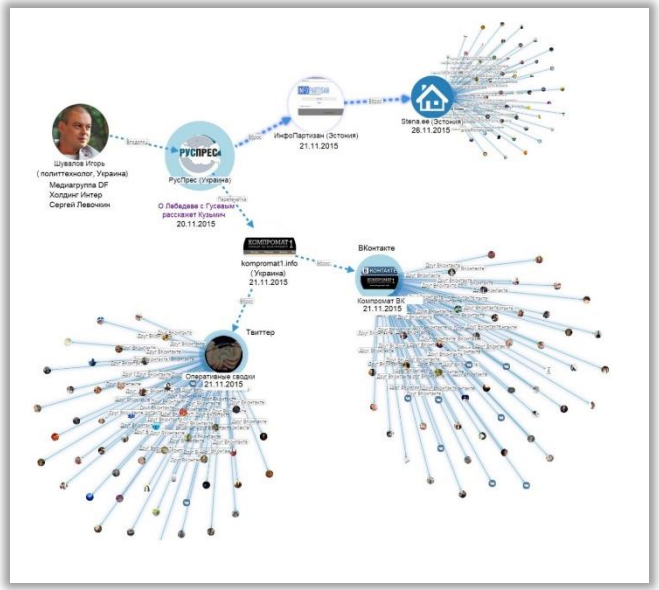
Cambridge Analytica





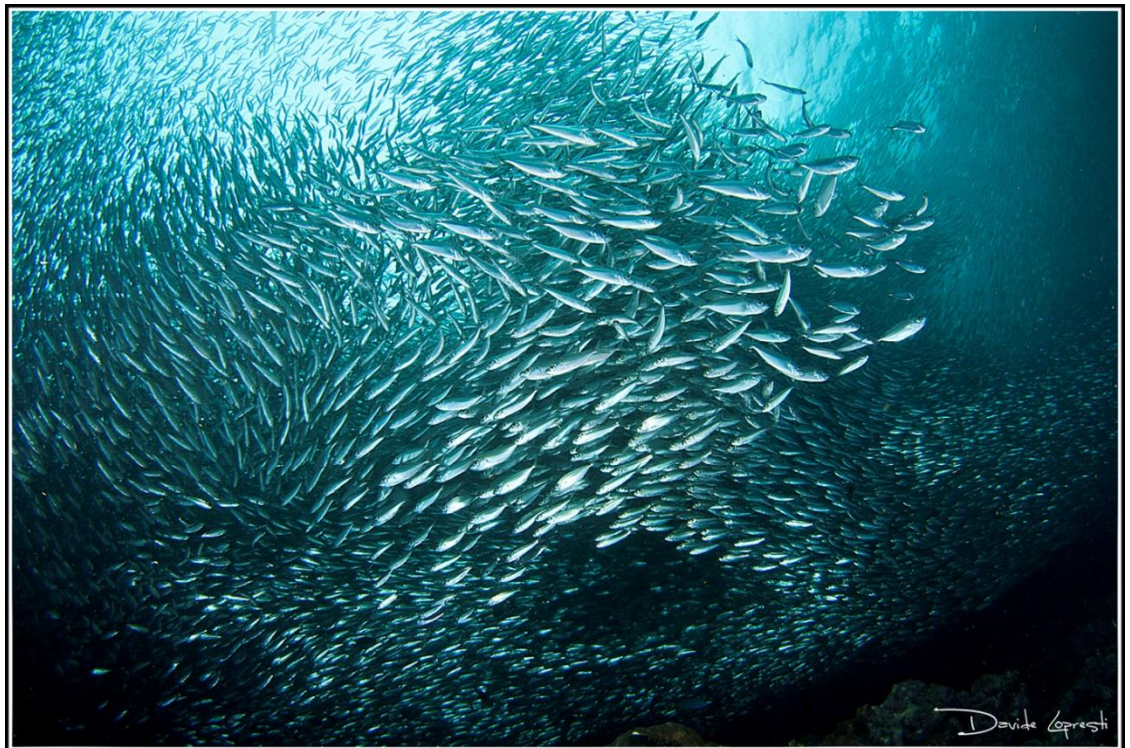
Step3: Action!



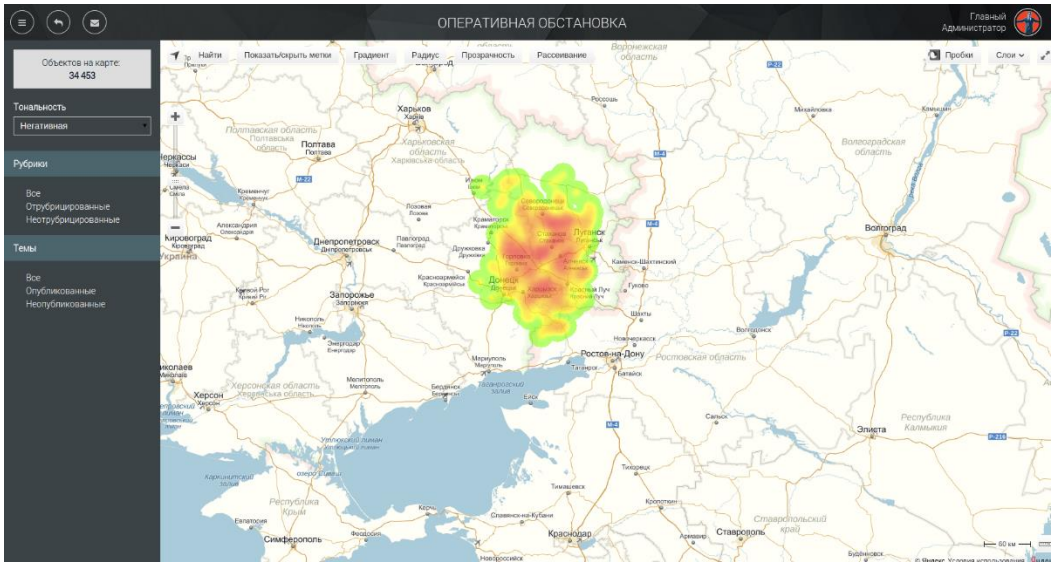


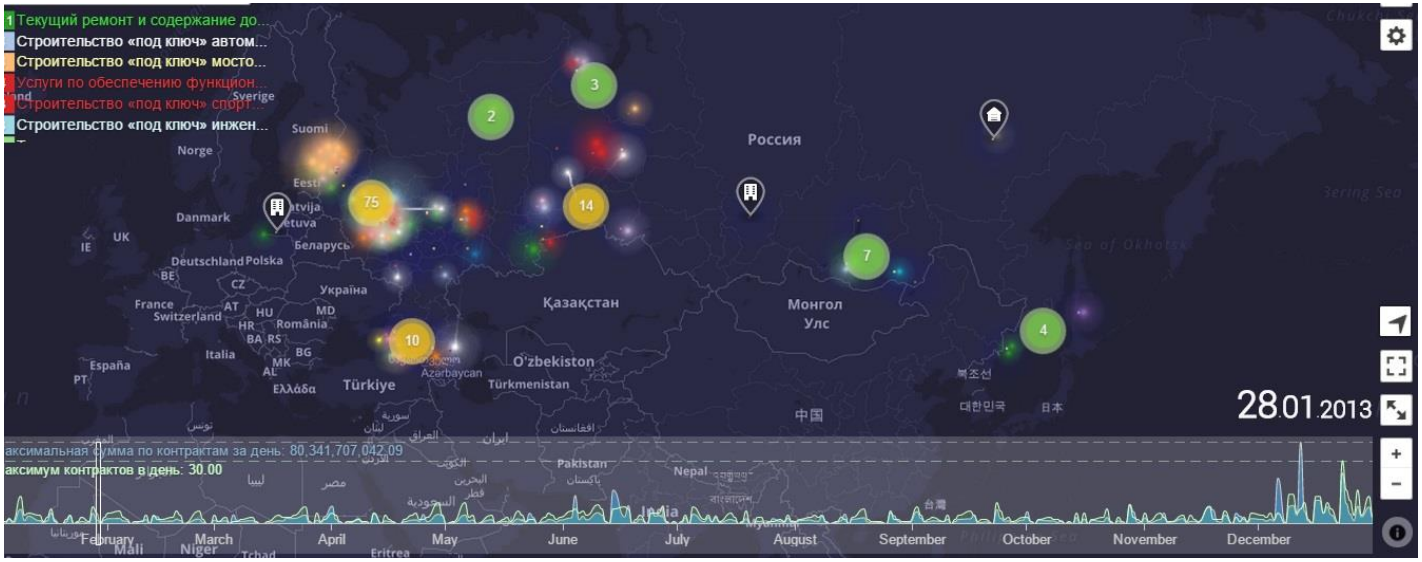
Вброс: этапы распространения

- Сначала – сеть подконтрольных ресурсов
- Затем – последователи (followers)
- Далее – очаги возбуждения в среде объектов воздействия



Тепловая карта активности в социальных сетях





Воздействие на массовое сознание – это вообще этично?

Освобождение Праги, 1945

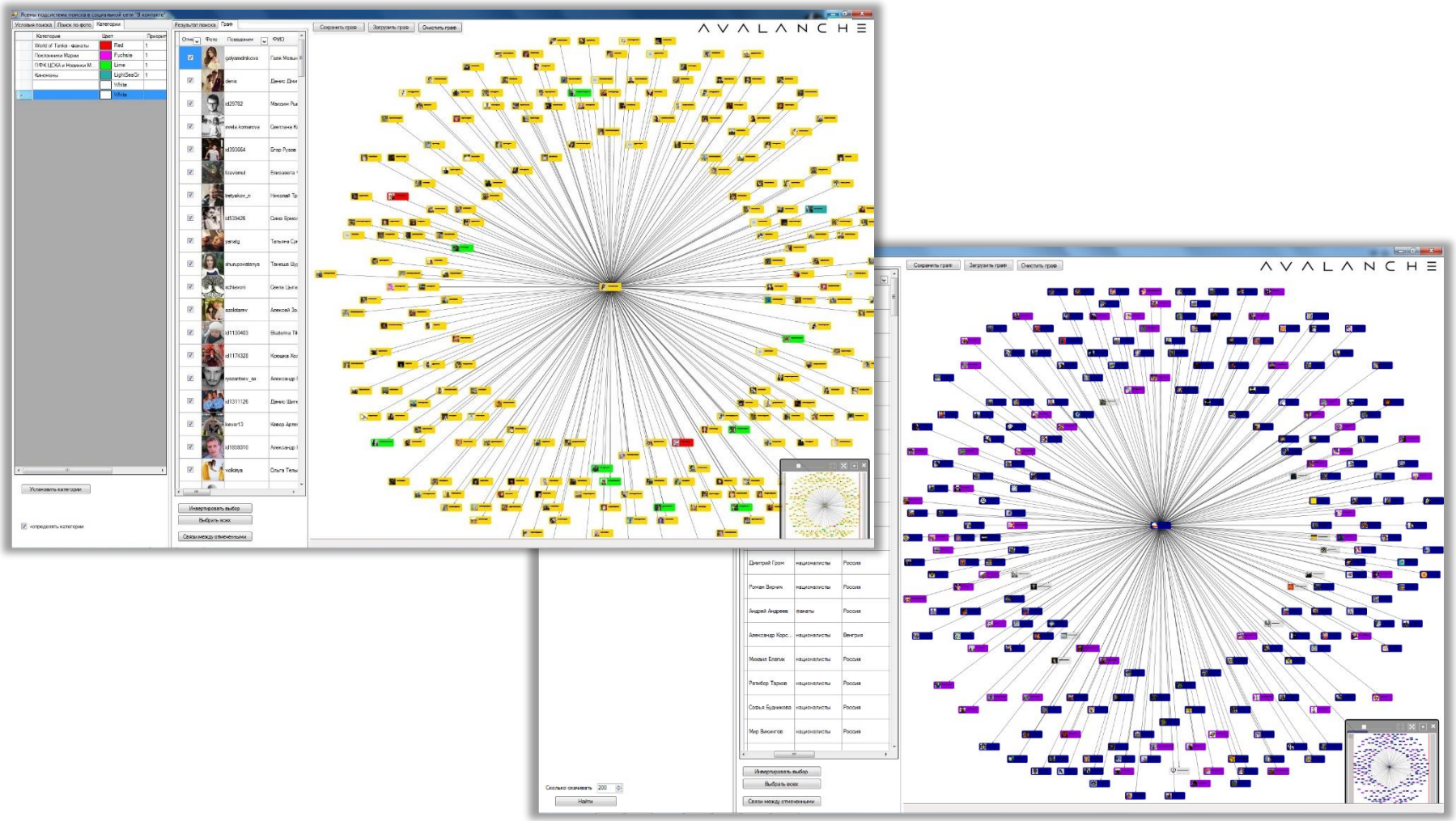
«Конвой свободы», 2017

Пора вмешиваться…

Освобождение Праги, 1945

«Конвой свободы», 2017

Экспресс-анализ социального здоровья аудитории



Елки-5: Боты против пиратов

В день выхода фильма «Елки-5» злоумышленники организовали массированное распространение ссылок на пиратскую копию фильма

Противодействие:

- «Поглощение» атаки
- Встречная атака
- «Бот-юрист»

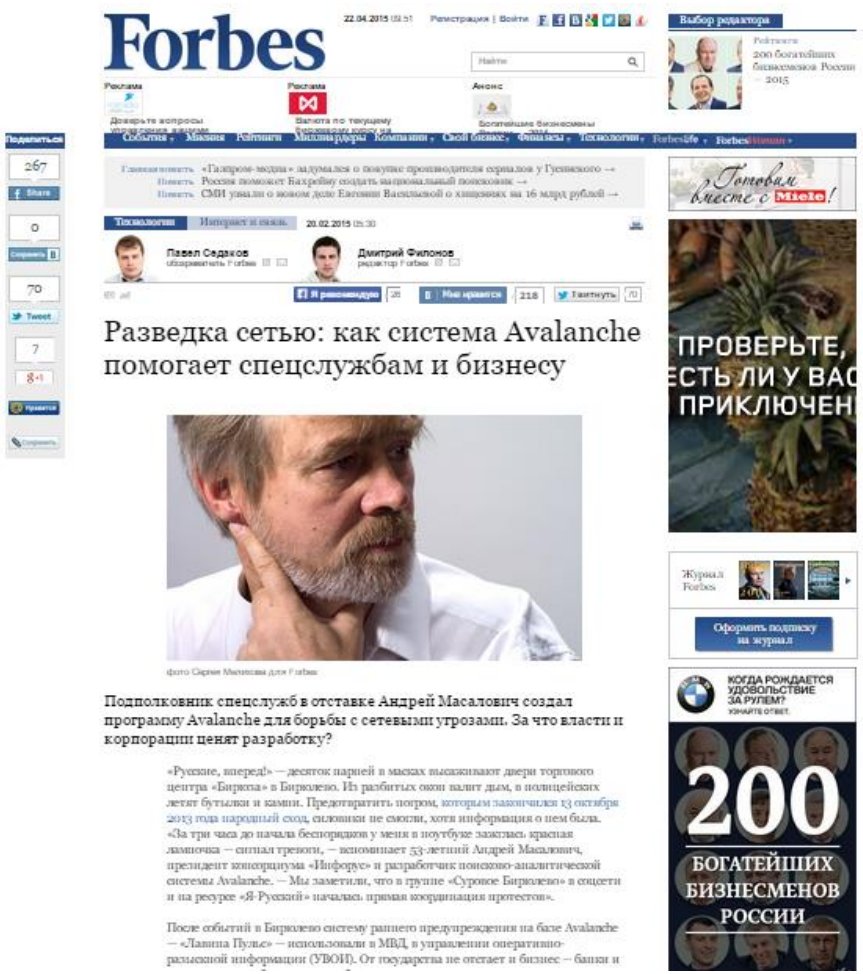
Пожар в Оптиной пустыни: Боты против мошенников

25 января 2017 года в 12.40 в женской общине в честь Святых жен-мироносиц с. Клыкова Козельской епархии произошел пожар.
Более 50 мошенников объявили в Сети о сборе средств

Противодействие:

- Бот «Совесть»
- Встречная атака
- «Бот-юрист»

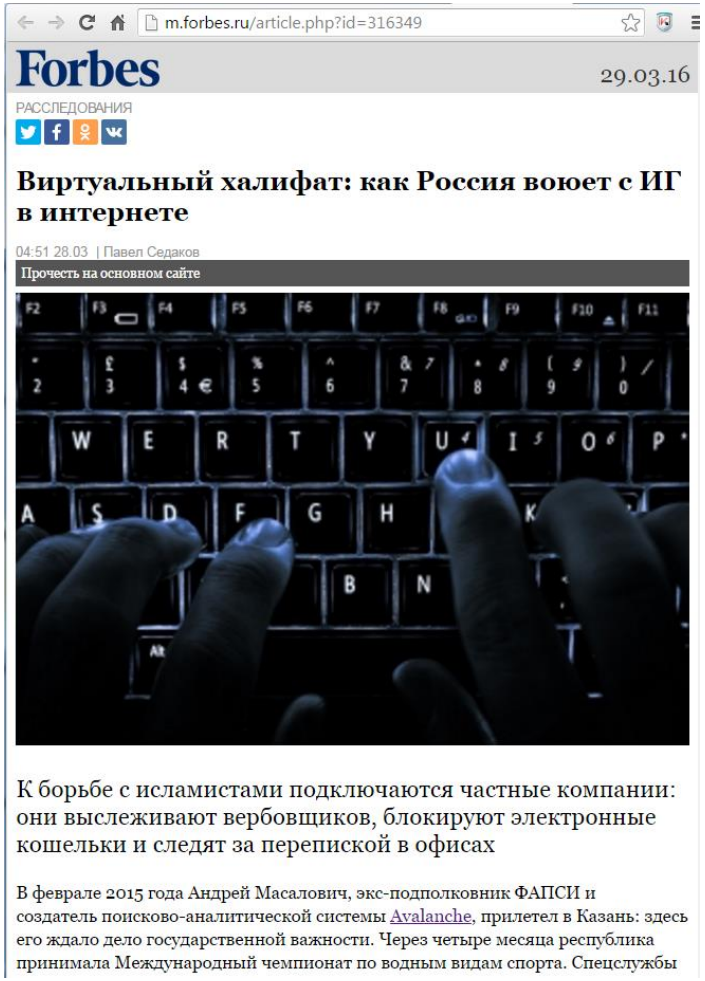
О поисковой технологии Avalanche: Forbes Russia N2, 2015 и др.



Forbes

Разведка сетью: как система Avalanche помогает спецслужбам и бизнесу

Подполковник спецслужб в отставке Андрей Масалович создал программу Avalanche для борьбы с сетевыми угрозами. За что власти и корпорации ценят разработку?



m.forbes.ru/article.php?id=316349

Forbes 29.03.16

РАССЛЕДОВАНИЯ

Виртуальный халифат: как Россия воюет с ИГ в интернете

04:51 28.03 | Павел Седаков

Прочесть на основном сайте

К борьбе с исламистами подключаются частные компании: они выслеживают вербовщиков, блокируют электронные кошельки и следят за перепиской в офисах

В феврале 2015 года Андрей Масалович, экс-подполковник ФАПСИ и создатель поисково-аналитической системы Avalanche, прилетел в Казань: здесь его ждало дело государственной важности. Через четыре месяца республика принимала Международный чемпионат по водным видам спорта. Спецслужбы

Спасибо за внимание ☺

iam.ru/tipaguru.htm

Masalovich Andrei
Масалович Андрей Игоревич
Специалист по связям с реальностью
+7 (964) 577-2012
am@avl.team