

-RUNET—ID-

eTicket

International forum
on practical information security

phd
Positive
Hack
Days

**ENEMY
INSIDE**
THE
STANDOFF

Krasnopresnenskaya emb. 12
May 23-24, 2017

Masalovich
Andrei

СПИКЕР

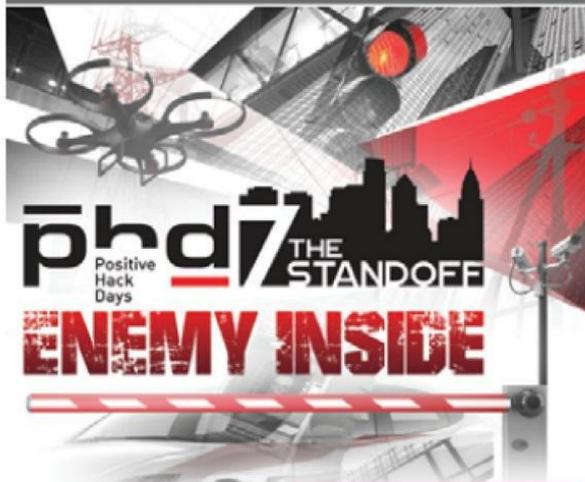


757308



To pass to the event You must present a ticket

-RUNET—ID-



Organizer — Positive Technologies

POSITIVE TECHNOLOGIES

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



@phdays

-RUNET—ID-



phdays.com
phdays.ru



WTC
MOSCOW



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

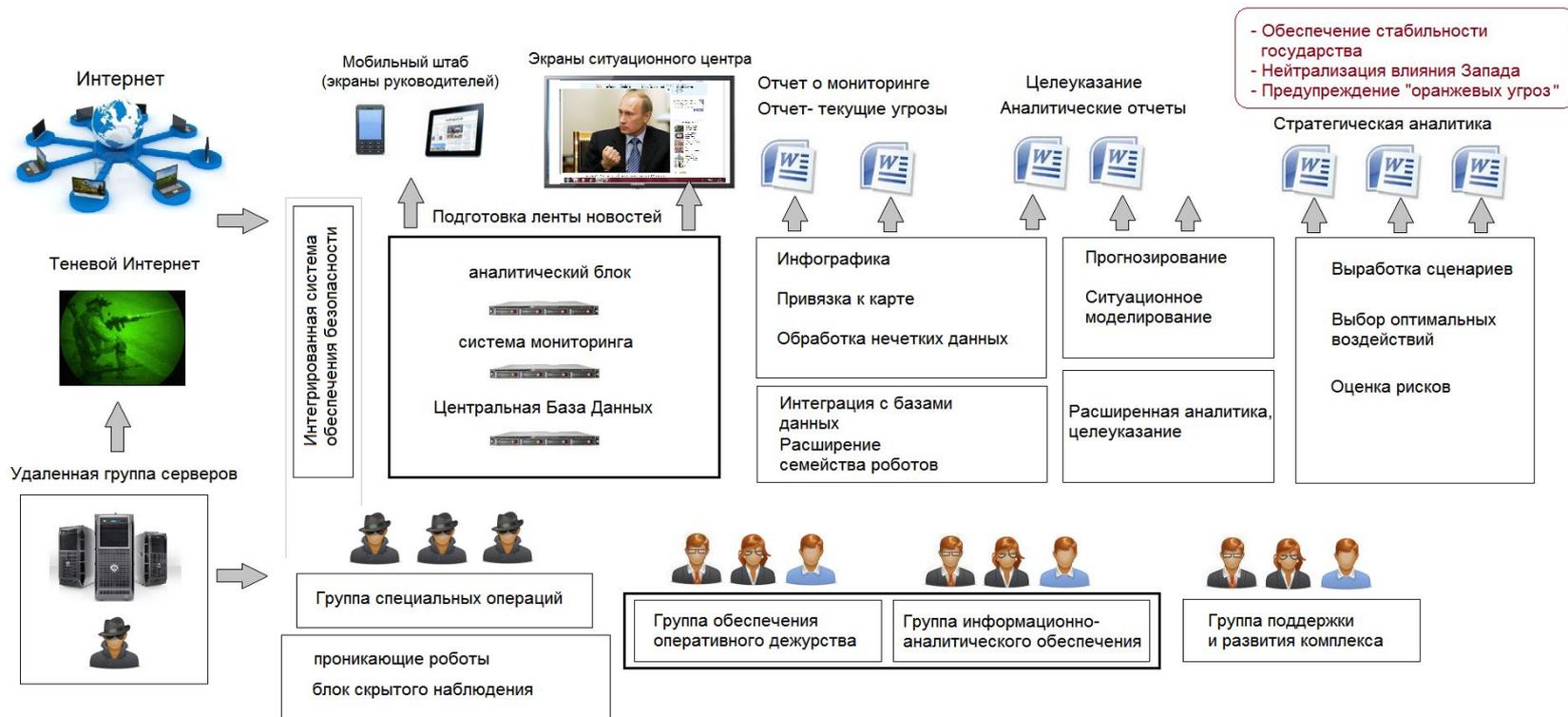
These days, the Web Standoff is not just a warfare between humans and bots, we are talking about a botnet programmed to act in an intelligent, user-like manner, an army with a proper coordination. DDoS botnets have evolved from a basic tool to a powerful weapon of information confrontation in the hands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

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

AVANCE

Технологическая платформа информационного противоборства

Структура программного обеспечения Ситуационного центра



НОВЫЙ ВЗГЛЯД НА ВЗЛОМ

The Hacker

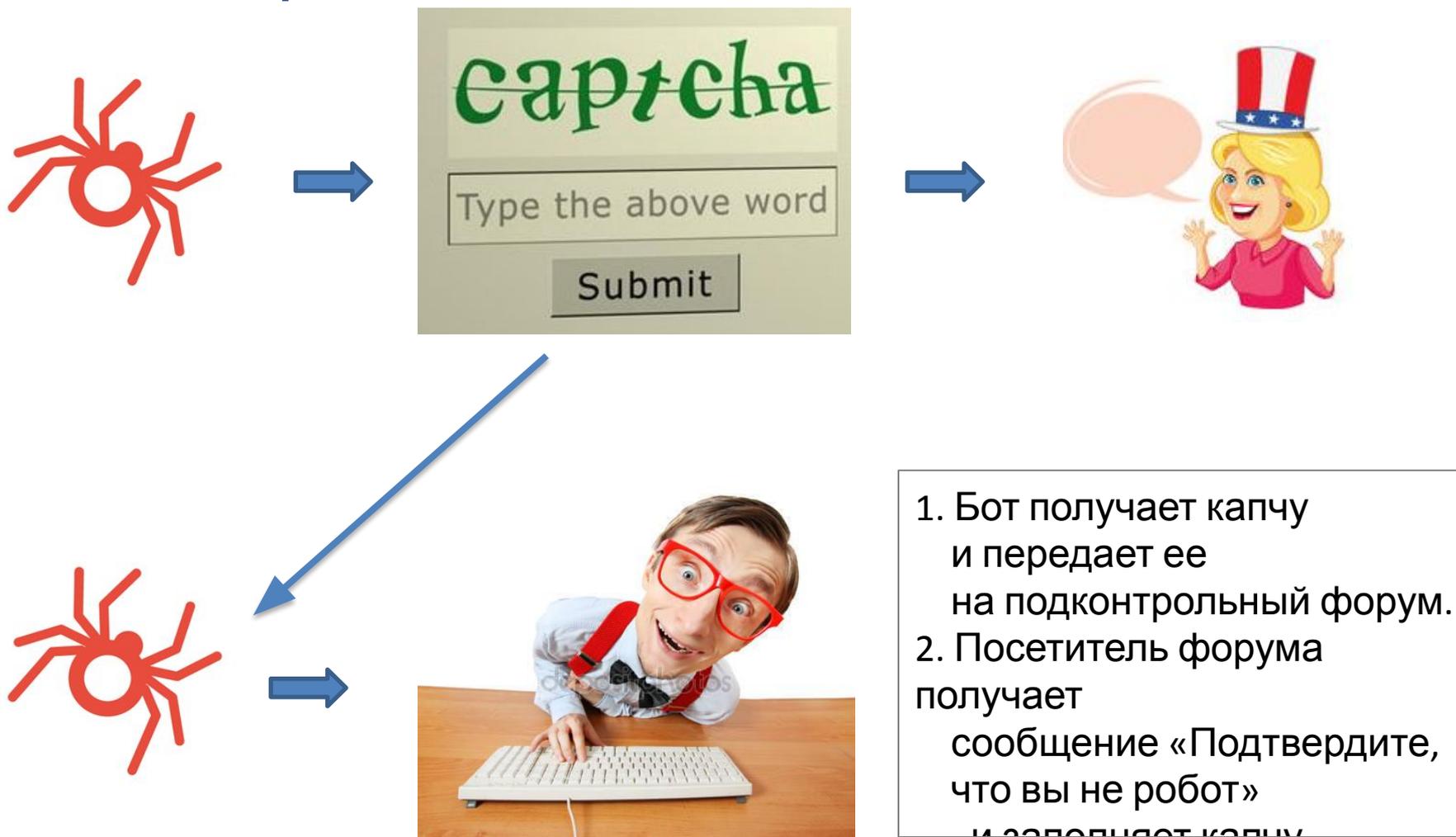


Definition - What does *Internet Bot* mean?

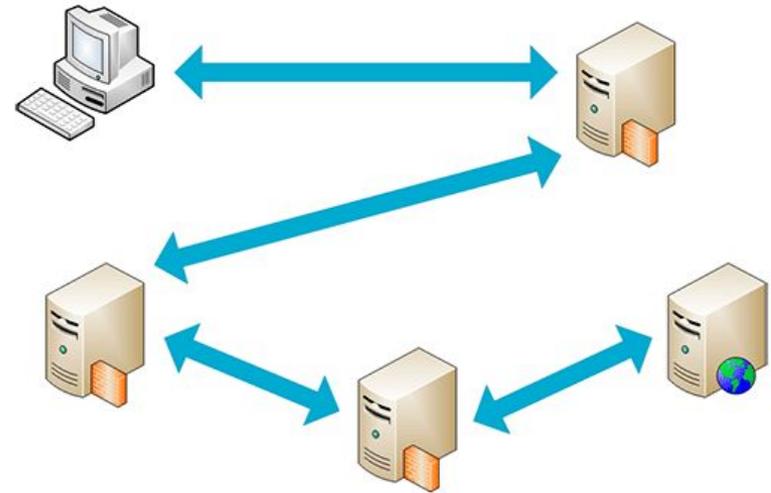
- **An Internet Bot**, also known as web robot, WWW robot or simply bot, is a software application that runs automated tasks (scripts) over the Internet.
- Typically, bots perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone.
- 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 Capcha

Обходим капчу: два бота и один хакер



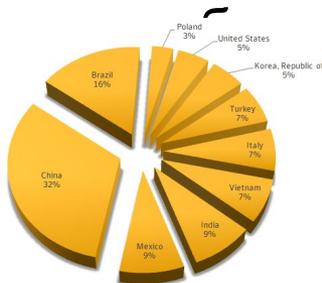
Guccifer 2.0 Hacked Clinton Foundation. How?



```
5 import todos from './ui/reducer';
6 import ui from './ui/reducer';
7 import users from './users/reducer';
8 import { LOGOUT } from './auth/actions';
9 import { UPDATE_APP_STATE_FROM_STORAGE_SUCCESS } from './app/actions';
10 import { combineReducers } from 'redux';
11 import { fieldsReducer as fields } from './lib/redux-fields';
12 import { firebaseReducer as firebase } from './lib/redux-firebase';
13 import { firebaseReducer as firebase } from './lib/redux-firebase';
14 import { routerReducer as routing } from 'react-router-redux';
15
16 //Guccifer 2.0 was here//
17
18 // Reset app state on logout, stackoverflow.com/q/35622588/233902.
19 const resetOnLogout = (reducer, initialState) => (state, action) =>
20   if (action.type === LOGOUT) {
21     // Delete whole app state except some fixtures and routing state.
22     state = {
23       device: initialState.device,
24       intl: initialState.intl,
25       routing: state.routing // Note routing state has to be reused.
26     };
27   }
```

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 очистки памяти
- Убивает уязвимый демон Telnet
- Просит администратора отключить уязвимую службу, сменить пароль



ить прошив

```
$ telnet [redacted]
Trying [redacted] ..
Connected to [redacted].
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.

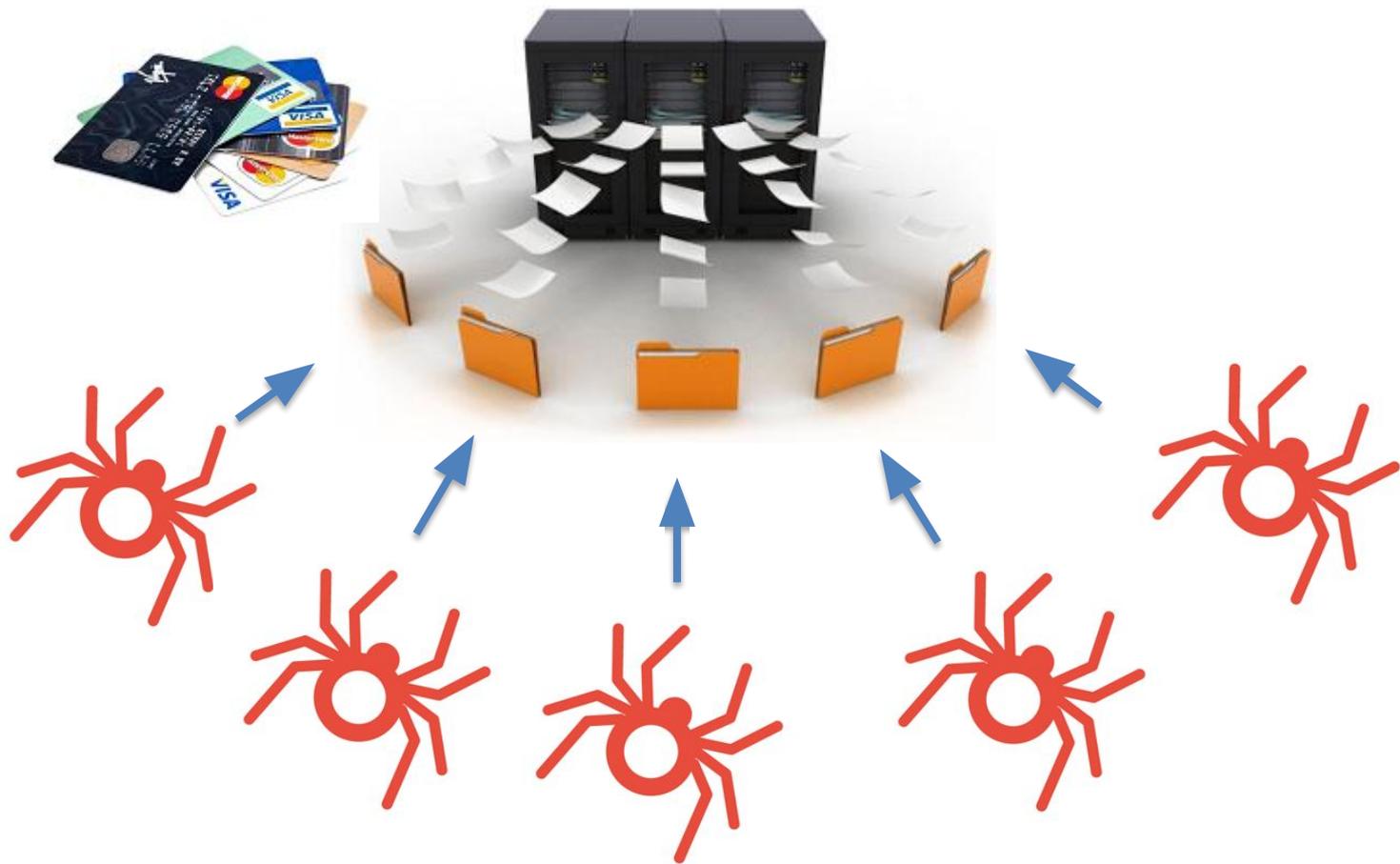
Connection closed by foreign host.
$
```

Does The Online Card Payment Landscape Unwittingly Facilitate Fraud?



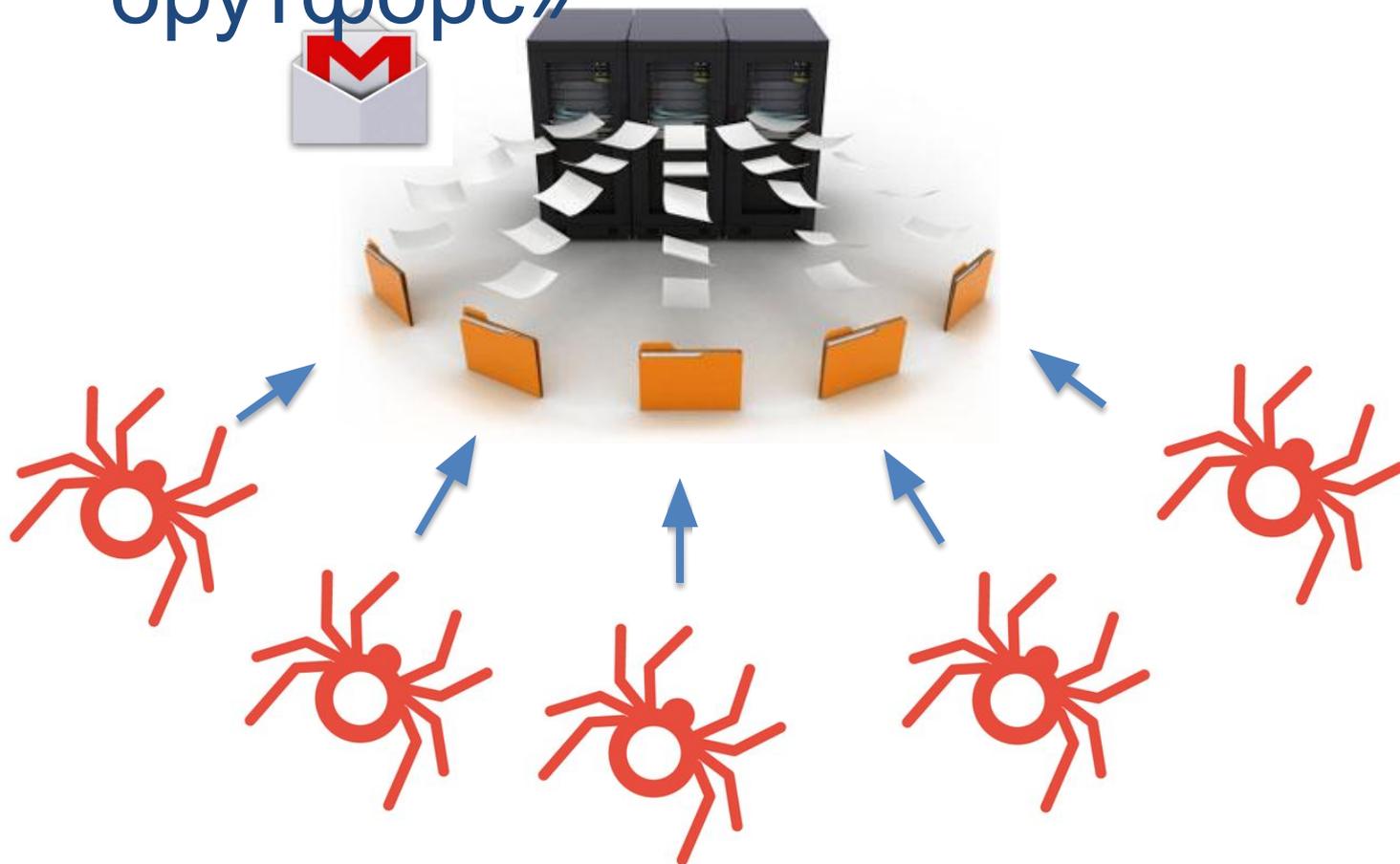
- 389 магазинов из ТОП-400 не препятствовали анализу защищенности
- 291 магазин проверяет всего три поля карты (номер карты, срок действия и CVV)
- 26 магазинов проверяют всего два поля карты
- Только 25 магазинов делают дополнительные проверки
- Только 47 используют технологию защиты 3-D Secure
- Бот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

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



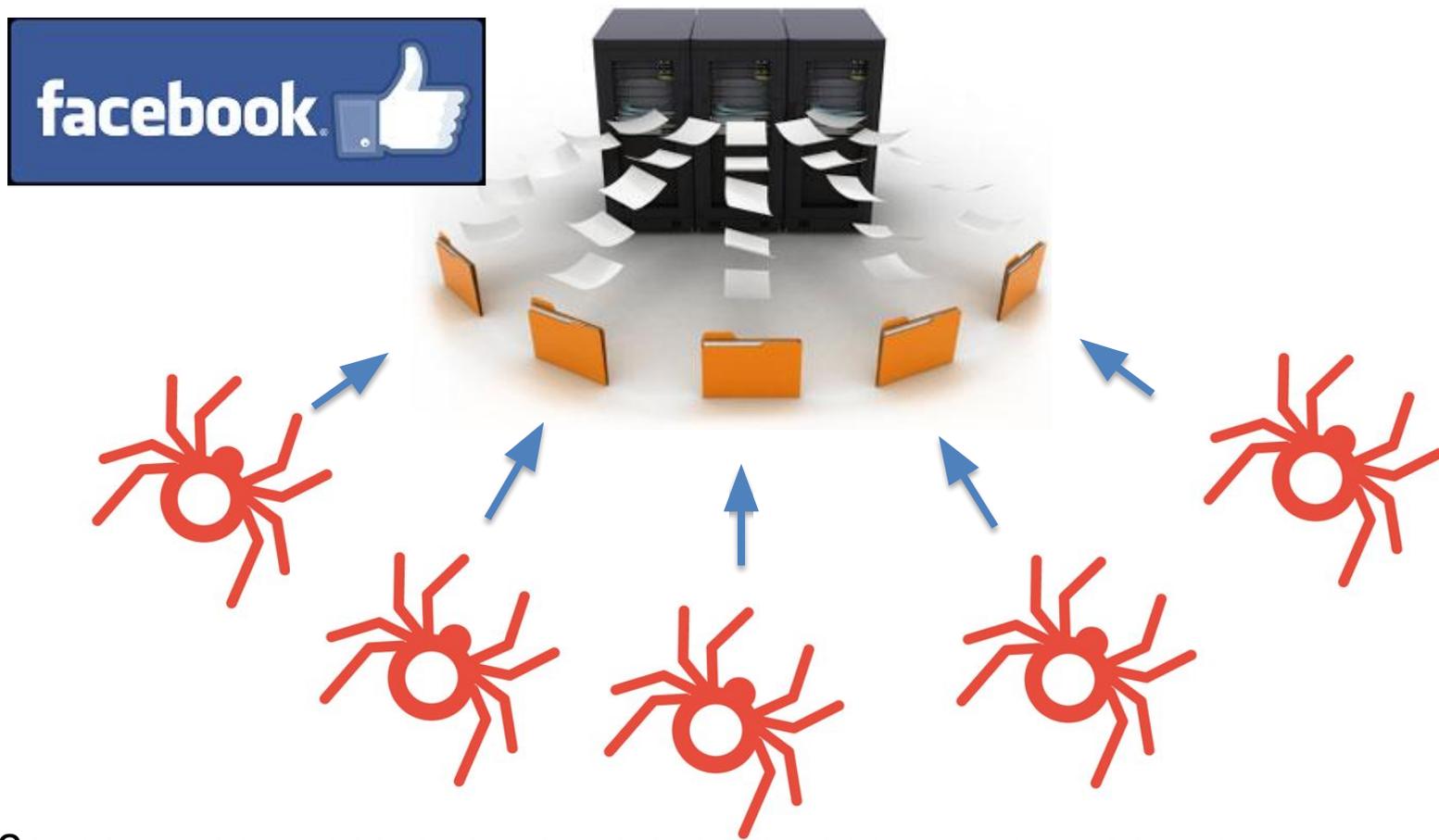
Multi-Login Brutforce: smart bots attack mail server

«Горизонтальный брутфорс»



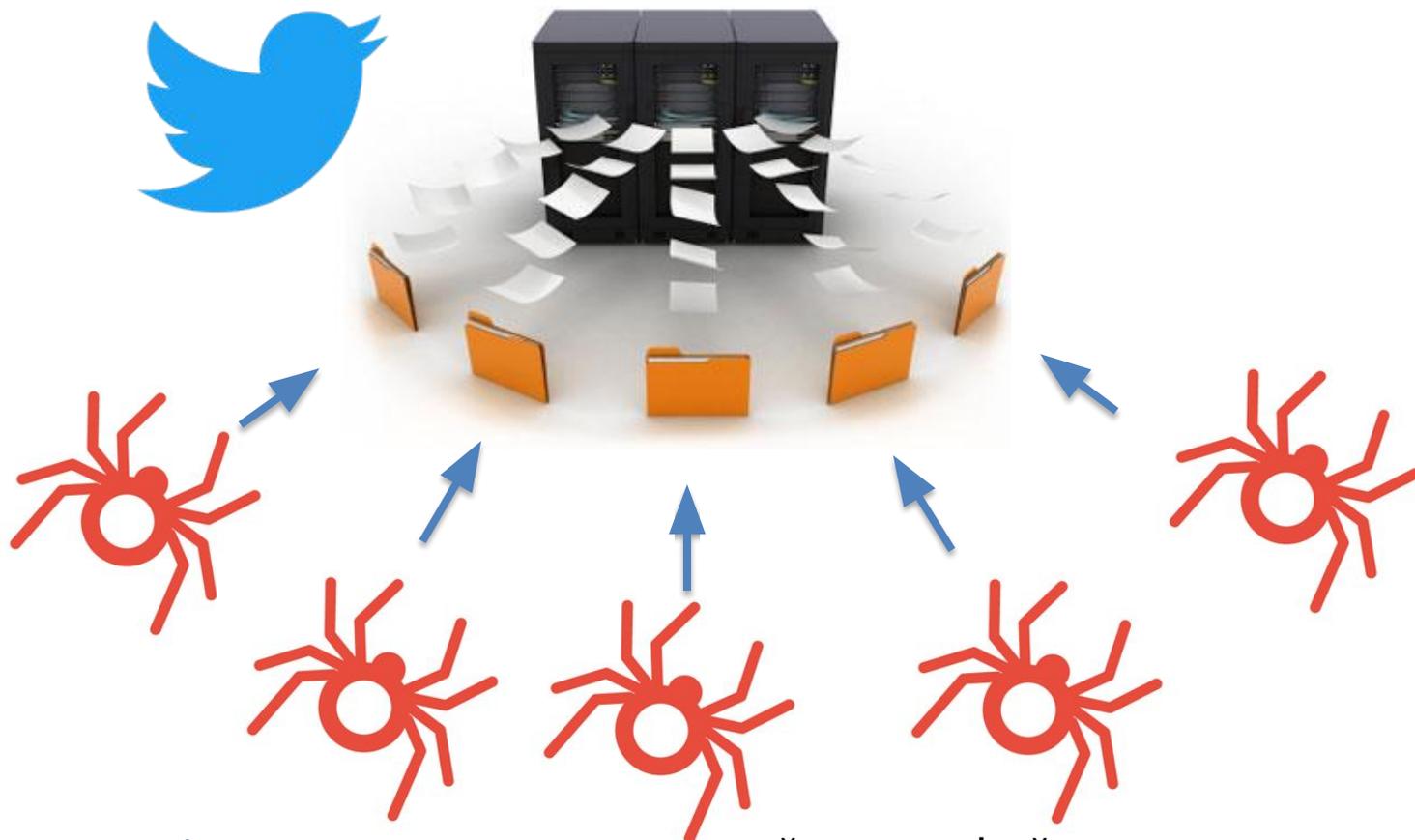
- Подбор паролей к заданному логину будет пресечен сразу
- Попытки зайти с одним паролем с тысяч логинов сервер не

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



1. Запрашиваем восстановление своего пароля – получаем код подтверждения
2. Запрашиваем восстановление пароля от имени миллиона подсерверов

How to crack Twitter



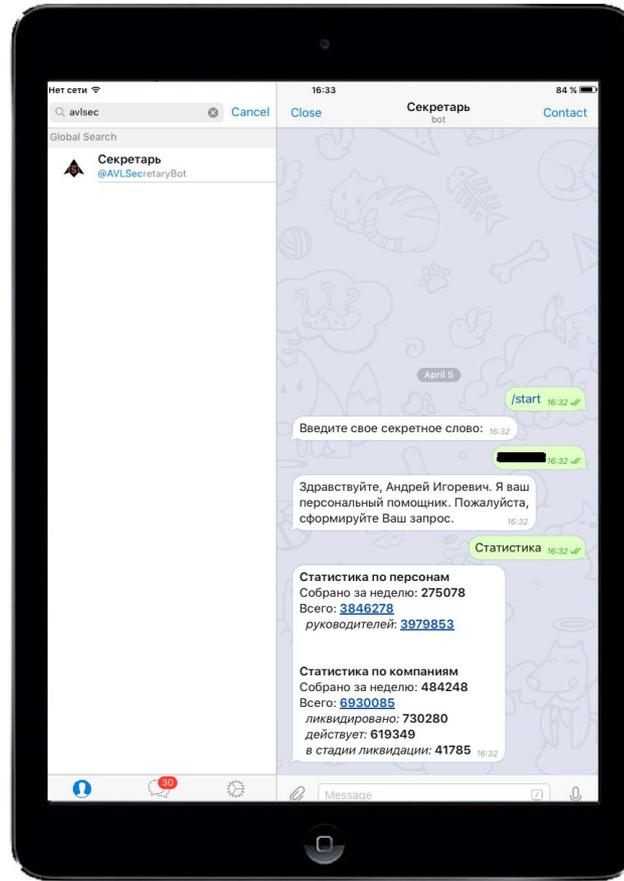
1. Заходим в ads.twitter.com, загружаем свой медиа-файл
2. Делимся этим файлом с аккаунтом жертвы
3. Перехватываем запрос публикации твита и подменяем в POST `owner_id` и `user_id` на id twitter аккаунта жертвы. Твит будет опубликован от его имени.

Источник:

<https://habr.com/ru/news/entries/237994/>

Новый взгляд на поисковые роботы и сканеры

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



А В А Л А Н Ч Е

WannaCry, prehistoria

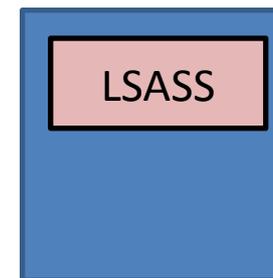
2004



139



445

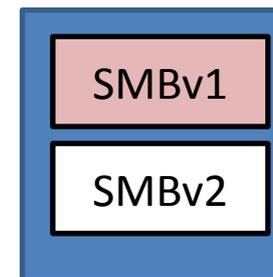


2006

139



445



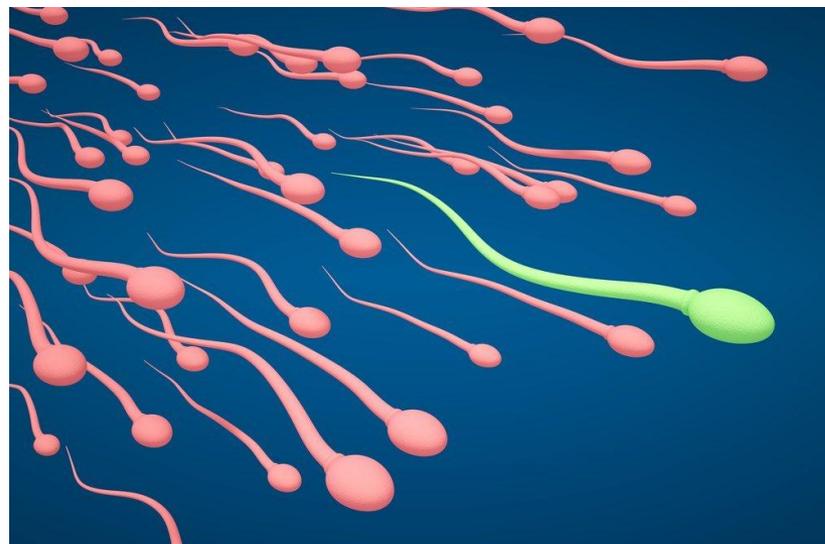
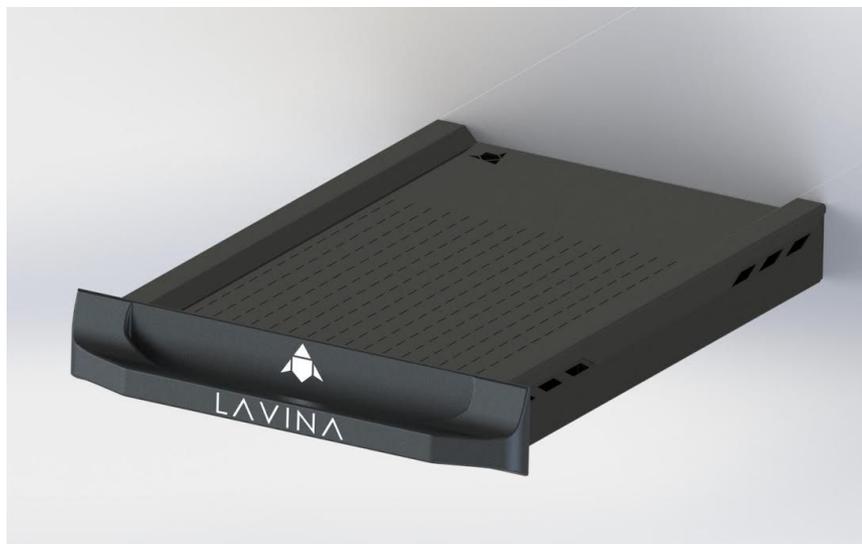
2017



Внешнее сканирование – вакцина от вирусов

Уроки WannaCry:

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



ЛАВИНА Сканер – активная защита нового поколения

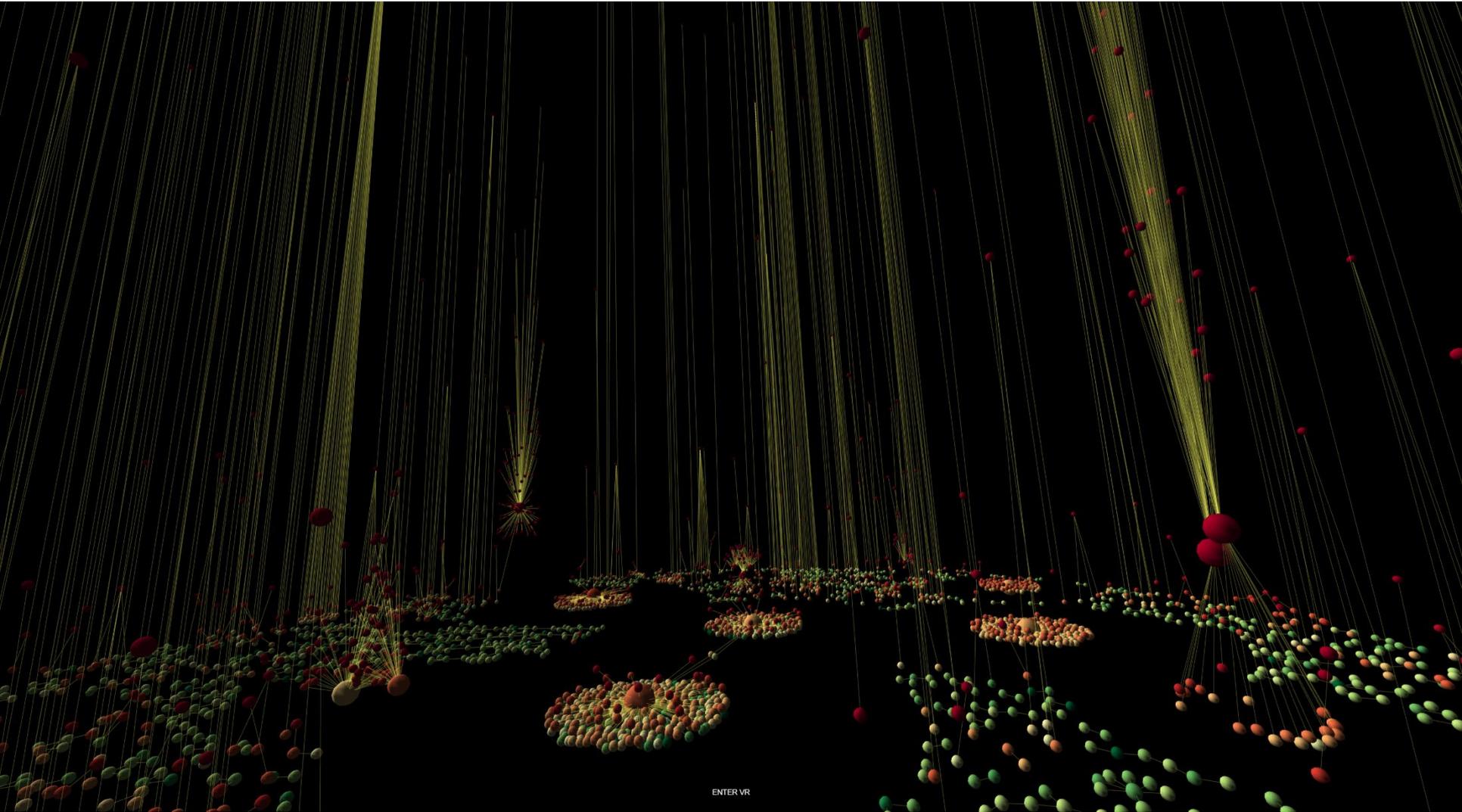
Новый взгляд на противоборство

Step to the Web



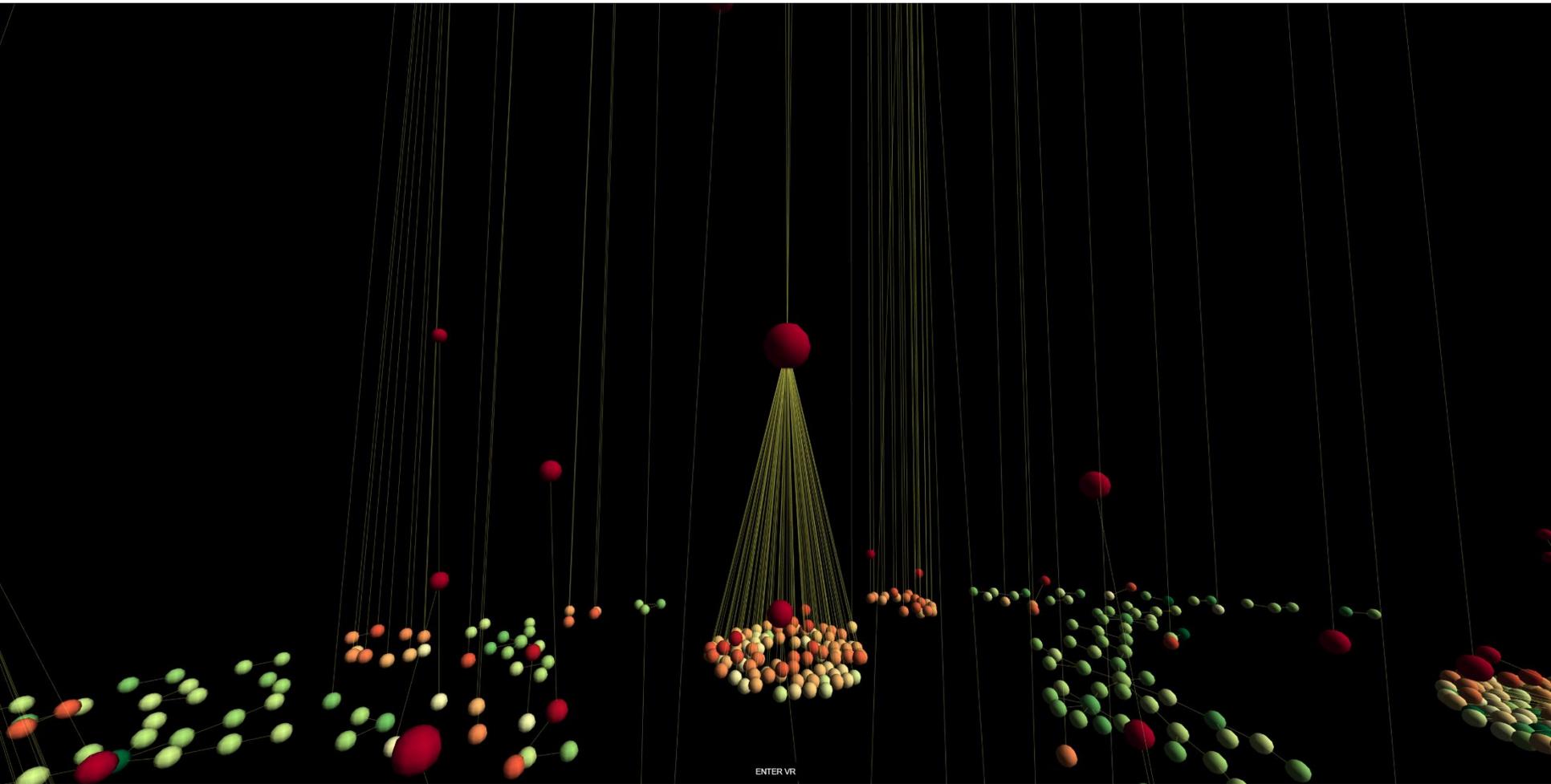
A V A L A N C H E

One minute inside Twitter



AVANCE

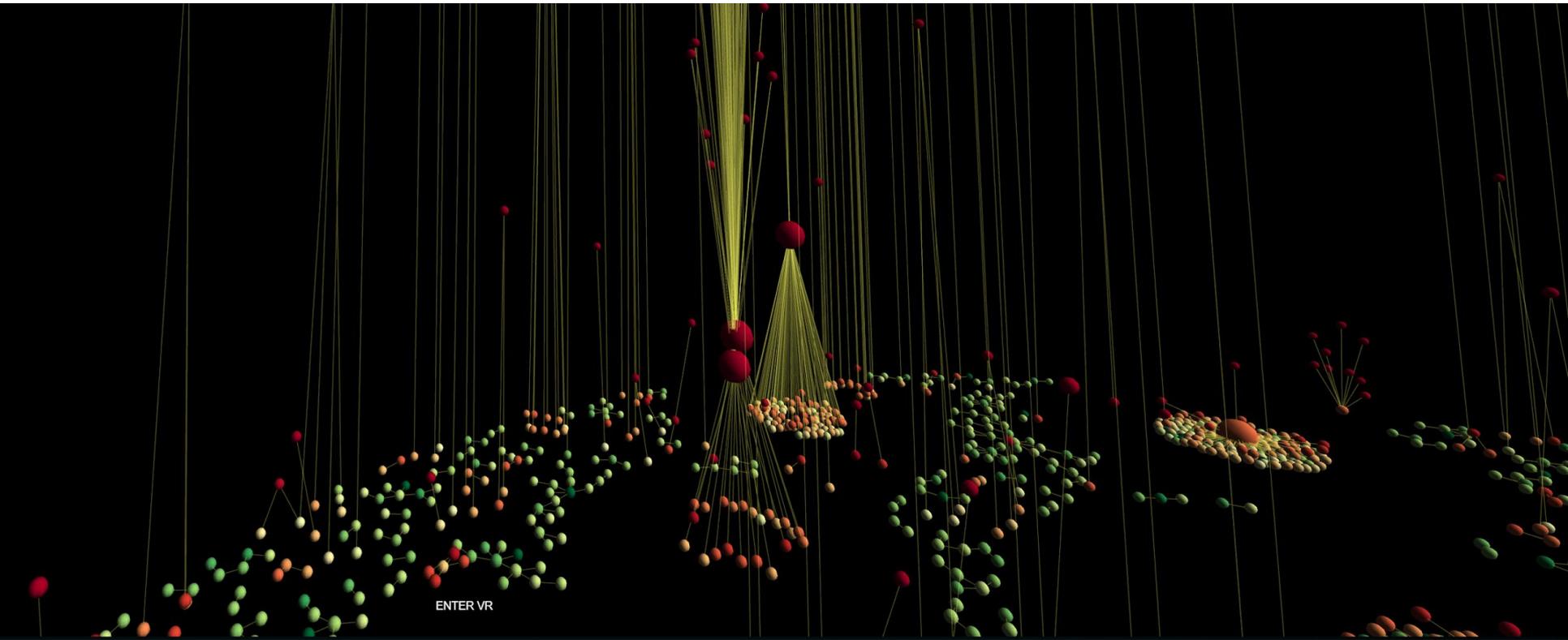
The Leader



ENTER VR

AVALANCHE

Real People vs Botnets



ENTER VR

^ V ^ L ^ N C H E

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

**IF THE RUSSIANS DID
ACTUALLY HACK THE ELECTION**

**\$8.4
BILLION**
2016 BUDGET



**\$9.88
BILLION**
2016 BUDGET



**\$44
BILLION**
2016 BUDGET



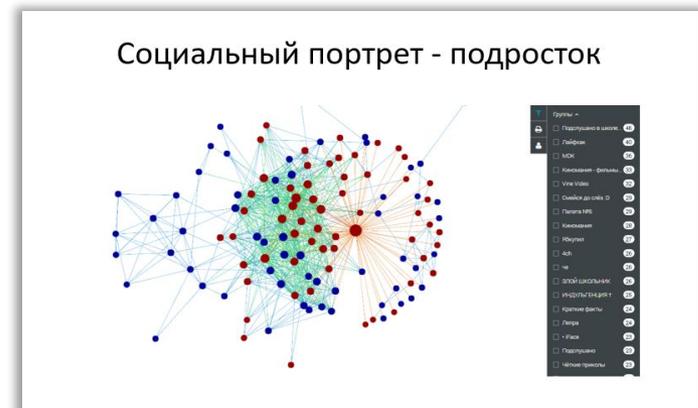
**WHAT THE HELL ARE
WE PAYING THESE GUYS FOR?**



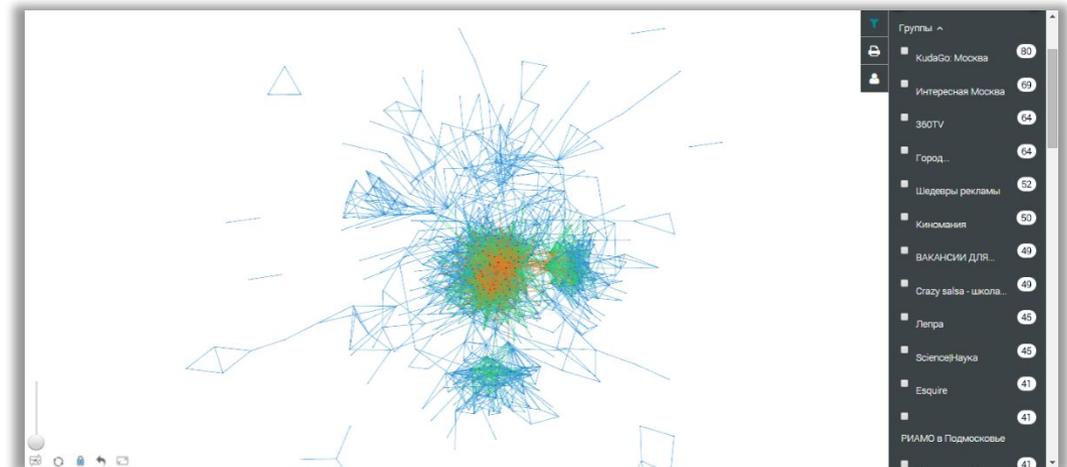
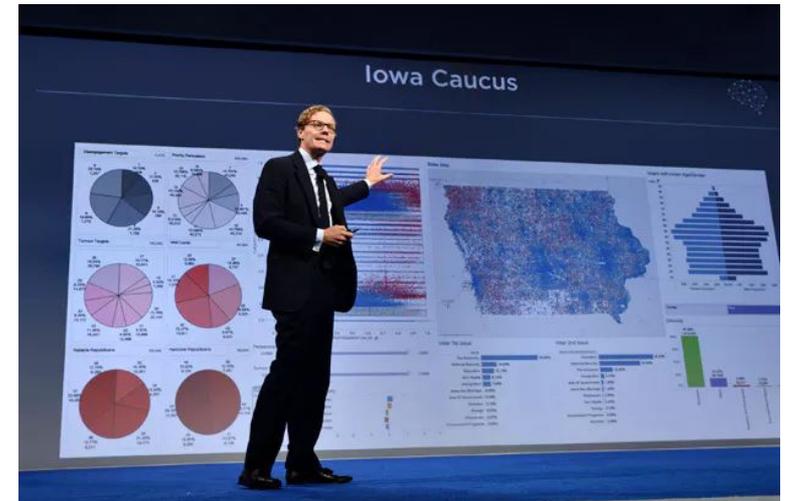
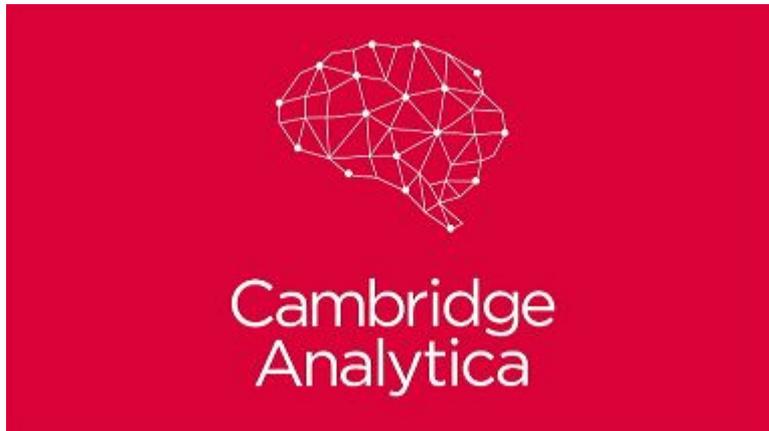
Step 1: Psychometrics

Psychometrics, a
data-driven
sub-branch of
psychology

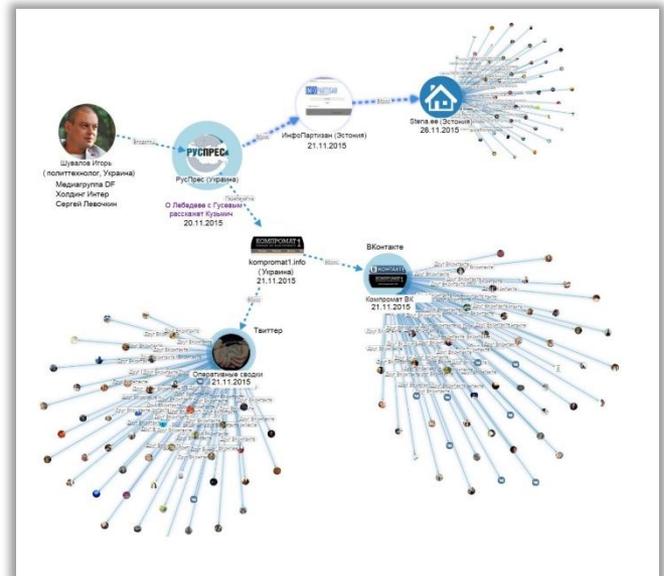
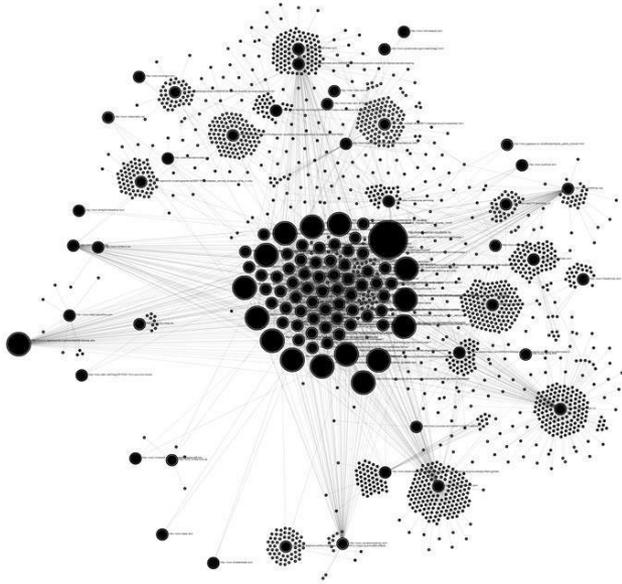
Анализа 68 лайков в Facebook
достаточно, чтобы определить цвет
кожи испытуемого (с 95%
вероятностью), его
гомосексуальность (88%
вероятности) и приверженность
Демократической или
Республиканской партии



Step 2: Better audience targeting

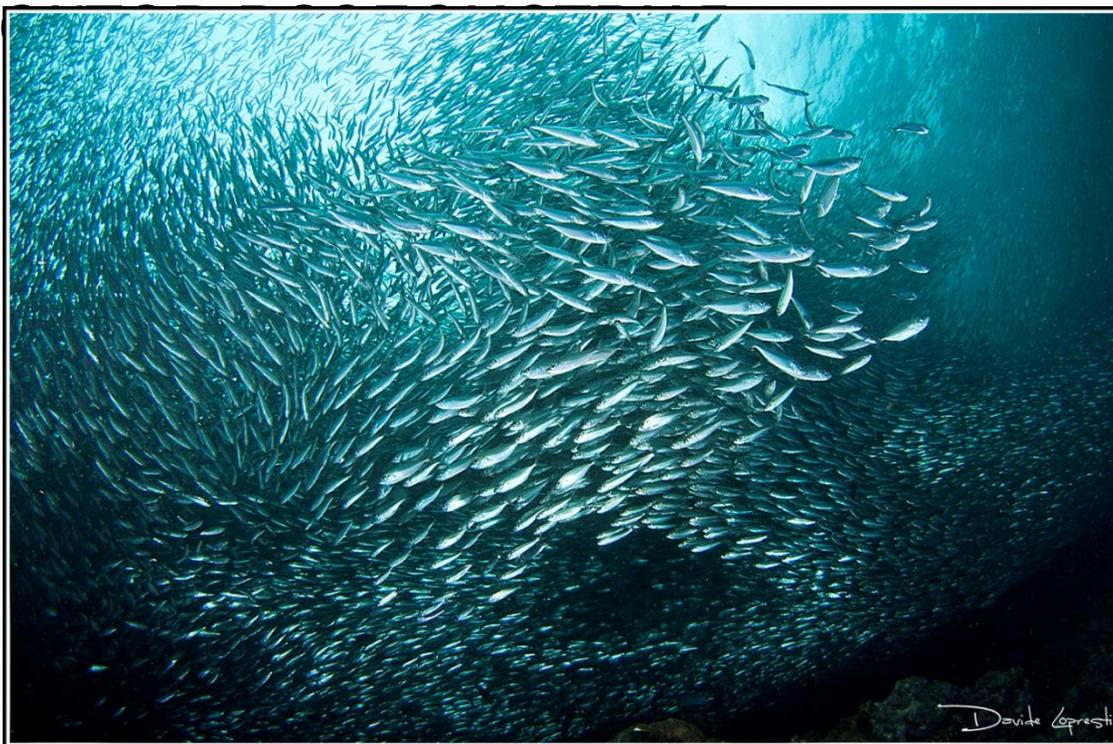


Step3: Action!

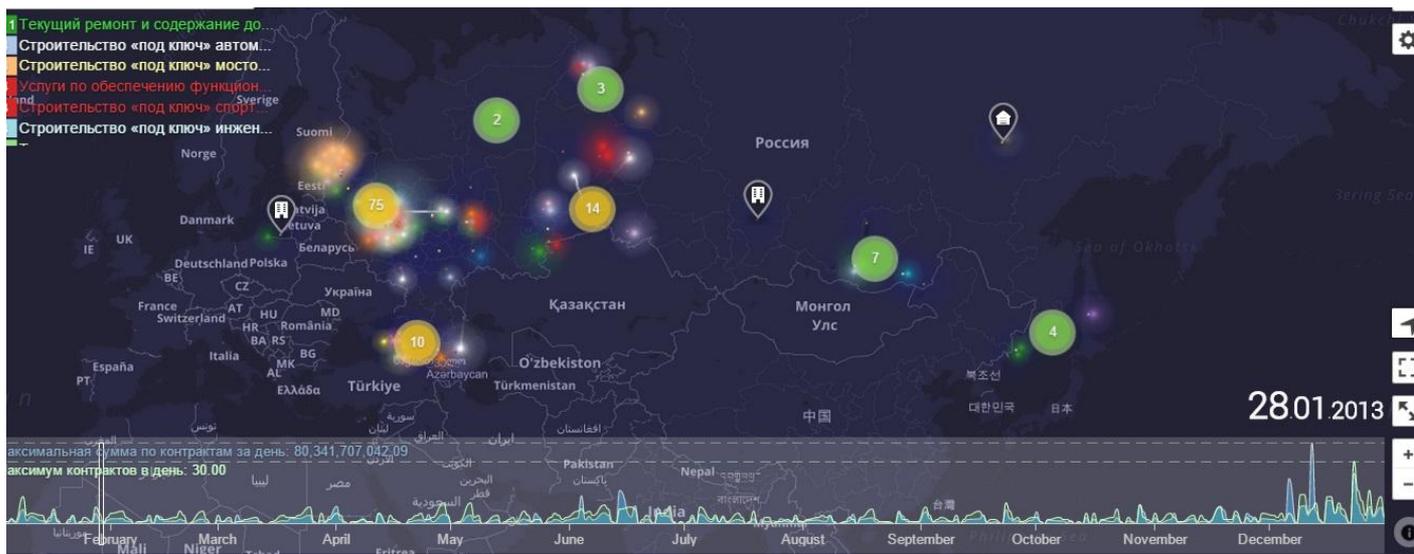
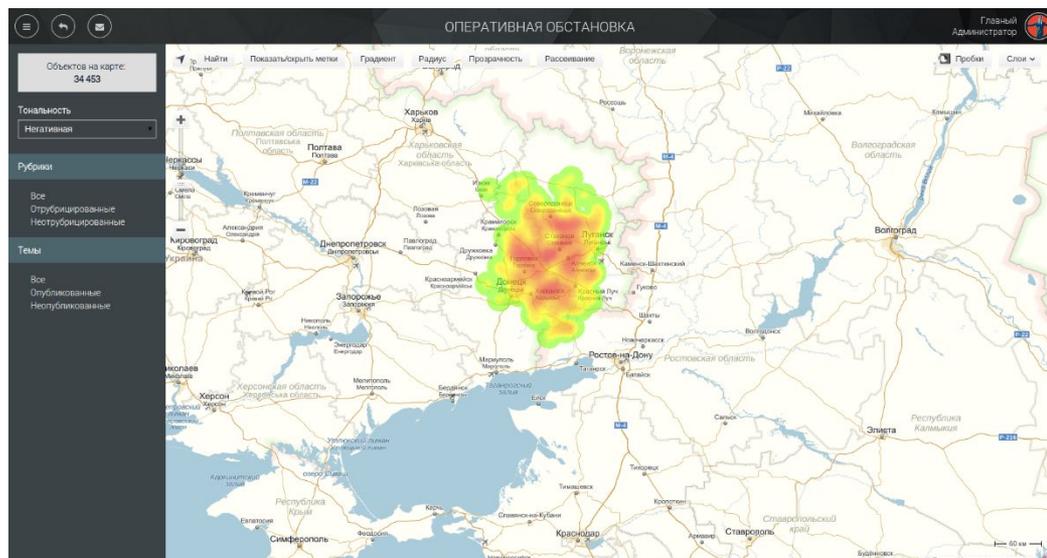


Вброс: этапы распространения

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



Тепловая карта активности в социальных сетях



Воздействие на массовое сознание – это вообще этично?



Освобождение Праги,
1945



«Конвой свободы»,
2017

Пора вмешиваться...

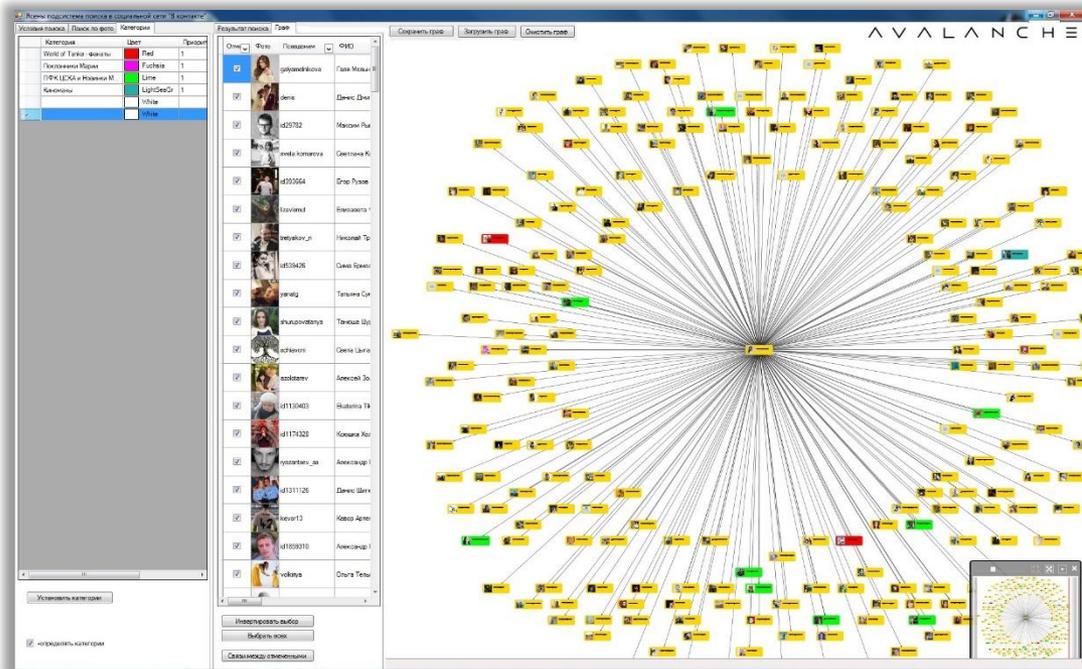


Освобождение Праги,
1945



«Конвой свободы»,
2017

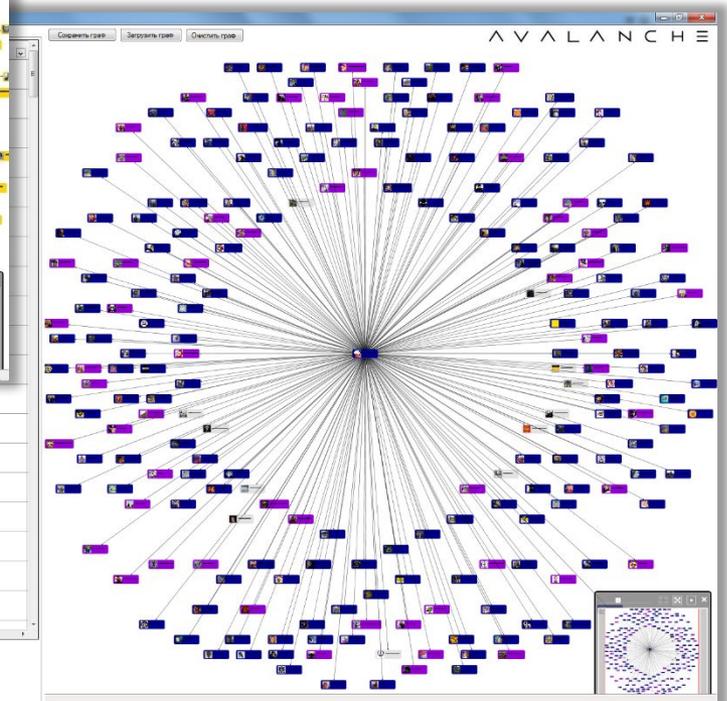
Экспресс-анализ социального здоровья аудитории



Дмитрий Гран	националисты	Россия
Роман Воронин	националисты	Россия
Андрей Андреев	нацбаты	Россия
Александр Корс	националисты	Венгрия
Михаил Елагин	националисты	Россия
Резибер Тархан	националисты	Россия
Светлана Бурденко	националисты	Россия
Мер Венигарт	националисты	Россия

Сколько отображать: 200
Найти

Интерпретировать выбор
Выбрать все
Связать между сгенерированными



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



Противодействи
е:

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

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



фото Сергея Митюшова для Forbes

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

«Русские, вперед!» — десктоп парней в масках высказывают двери торгового центра «Бирюза» в Бирюлево. Из разбитых окон валит дым, в полицейских летят бутылки и камни. Предвещать погром, которым закончился 13 октября 2013 года народный сход, силковик не смогло, хотя информация о нем была. «За три часа до начала беспорядков у меня в ноутбуке зазвонил красный лампочка — сигнал тревоги, — вспоминает 53-летний Андрей Масалович, президент концорсиума «Информ» и разработчик поисково-аналитической системы Avalanche. — Мы заметили, что в группе «Суровое Бирюлево» в соцсети и на ресурсе «Я-Русский» началась прямая координация протестов».

После событий в Бирюлево систему раннего предупреждения на базе Avalanche — «Лавина Пульс» — использовали в МВД в управлении оперативно-разыскной информацией (УОИР). От государства не отстает и бизнес — банки и

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 😊



Masalovich Andrei
Масалович Андрей
Игоревич

Специалист по связям с
реальностью

+7 (964) 577-2012

am@avl.team

iam.ru/tipaguru.htm