Personal security

Личная информационная безопасность

Активы и угрозы

- Данные
  - учетные данные к различным ресурсам
  - данные, идентифицирующие личность (ПД)
  - сведения о деятельности и активах личности (в т.ч. социальные связи)
  - собственные данные (фотки, доки, программы)
  - чужие данные (данные работодателя, клиентов)
- Угрозы
  - кража / потеря данных
  - обнародование (частный случай кражи) - в контексте атаки на репутацию

Brainstorming session: вектора доступа

- Кража у-ва (телефона, ноутбука)
- Взлом у-ва (телефона, ноута, PC, WiFi-роутера)
- Перехват данных в момент передачи (WiFi)
- Работа из недоверенных мест (Интернет-кафе)
- Взлом сервиса с данными
- Взлом сервиса, на котором зарегистрирован субъект
- Взлом учетной записи через уязвимость в сервисе
- Социальная инженерия (цели атаки / ее окружения)

… а теперь системнее

Точки входа для доступа к данным

- Клиентские устройства
  - телефоны, laptop’ы, wifi-маршрутизаторы
- Server side
  - сервисы с данными пользователя, сервисы, на которых зарегистрирован пользователь, сервисы, которые посещает пользователь
- Недоверенная инфраструктура (оконечная / сетевая)
  - wifi-сети, Интернет-кафе, работа, etc...
- Человеческий фактор
  - сам субъект, его близкое окружение

Клиентские устройства

- Кража
  - телефона, ноутбука, флешки
- Взлом у-ва
  - “добровольная” установка ВПО (scareware, false updates, прочая социалочка)
  - эксплойты в Интернет (java/flash/pdf/office/браузеры)
  - другие эксплойты (на флешках, в сетевых сервисах и т.п.)
  - закладки в ПО (кряки, кейгены, мобильные приложения и пр.)
  - подбор пароля к WiFi-маршрутизатору
  - прочие эксплоиты

Server side

- Взлом сервиса через серверную уязвимость
  - почтового, социальной сети, файлообменника (сканы паспорта), фотохостинга, Интернет-магазина
- Взлом учетки пользователя на целевом сервисе
  - XSS, CSRF, подбор пароля
- Взлом стороннего приложения или учётки пользователя на нем
  - например, почты, а потом восстановить пароль
  - или дырявого форума: пароли-то поди везде одинаковые

Недоверенная инфраструктура

- Оконечная
  - “брателло, дай почту с твоего компа проверить”
  - Интернет-кафе
  - после работы вашей мамы компьютер можно считать недоверенным
  - (возможно) работа
  - оставили у-во без присмотра и не ликвидировали риски? pwned
- Сетевая
  - открытые WiFi-сети
  - закрытые Wifi-сети с общим секретом
  - проводная инфраструктура в отелях, на работе
  - домашние локальные сети в некоторых конфигурациях

Человеческий фактор

- Фишинг (сайт выглядит также/похоже, но на другом домене, также похожем)
- Выманивание информации
- Одинаковые/похожие пароли и другие секреты
- Публикация данных о себе (прочих секретов, например, написать пароль на стикере)

Проблема сервиса или пользователя?

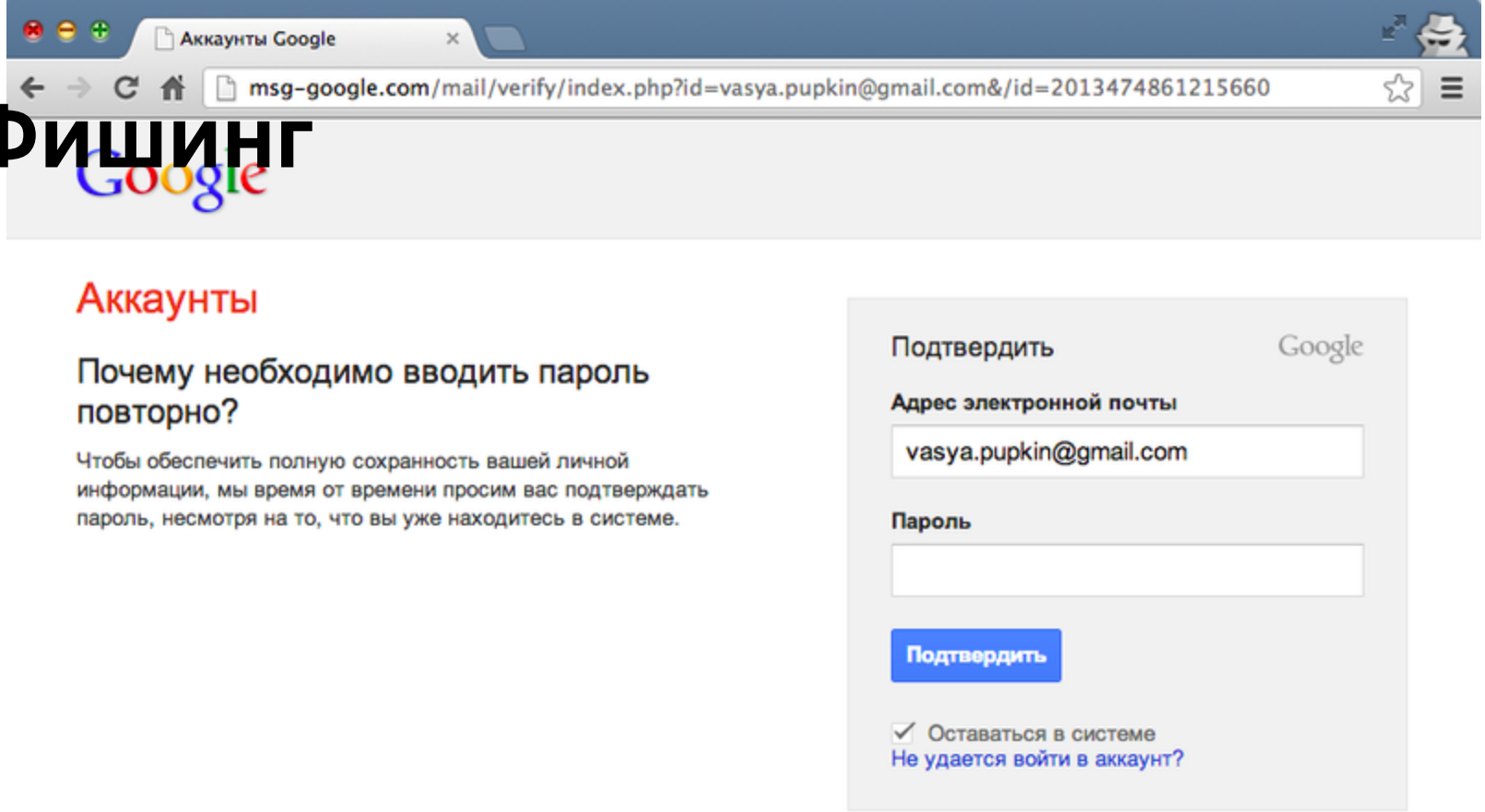
Anton Karpov
@toxo4ka

Following

Во всех сервисах регистрации контрольные вопросы по-прежнему задают на выбор такие, которые отлично бьются по профилям соцсетей. Доколе?

Выманивание информации

Фишинг


Аккаунты Google
msg-google.com/mail/verify/index.php?id=vasya.pupkin@gmail.com&/id=2013474861215660
Google
Аккаунты
Почему необходимо вводить пароль повторно?
Чтобы обеспечить полную сохранность вашей личной информации, мы время от времени просим вас подтверждать пароль, несмотря на то, что вы уже находитесь в системе.
Подтвердить
Google
Адрес электронной почты
vasya.pupkin@gmail.com
Пароль
Подтвердить
Оставаться в системе
Не удается войти в аккаунт?

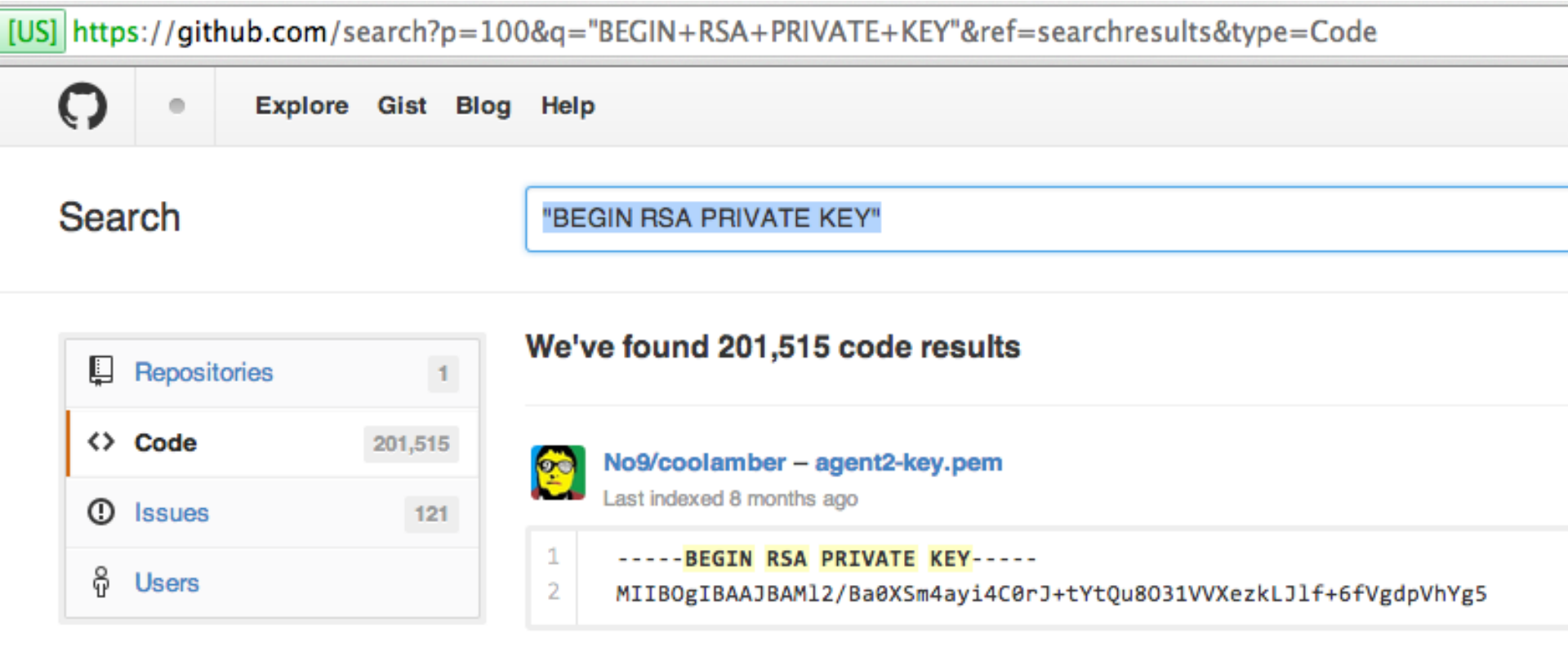
WORST PASSWORDS OF 2013

rank	password	change from 2012
#01	123456	⇈1
#02	password	⇊1
#03	12345678	—
#04	qwerty	⇈1
#05	abc123	⇊1
#06	123456789	new
#07	111111	⇈2
#08	1234567	⇈5
#09	iloveyou	⇈2
#10	adobe123	new

legend:
unchanged — up ⇈# down ⇊#

source data from splashdata

Публикация секретов



Одинаковые и похожие пароли

http://contest-2010.korelogic.com/rules.html

http://openwall.info/wiki/john/rules

Перебирать пароль выгоднее на самом слабом сервисе

Остальные методом индукции

Next time - меры противодействия