№205

ФЕВРАЛЬ 2016

ВЗЛОМ SINGLE SIGN-ON

ПЕНТЕСТИМ ВЕБ-АППЛИКУХИ НА БАЗЕ SAML SSO

Cover Story

Создаем свой Cydia-репозиторий

Прокачиваем Nmap скриптами на NSE

Делаем логгер звонков на Android

февраль 2016
№ 205

CONTENT

MEGANEWS
Всё новое за последний месяц

НЕБЕЗОПАСНАЯ АУТЕНТИФИКАЦИЯ
Ищем баги в приложениях с Single Sign-On на базе SAML

МОЗГИ НАПРОКАТ
Как сделать нейросеть или воспользоваться чужой

ВСЕ СВОЕ НОШУ С СОБОЙ
Обзор Remix OS — десктопной ОС на основе Android

КРАСНЫЙ ШУМ
Скрываем сетевую активность от продвинутой слежки

WWW2
Интересные веб-сервисы

NETFLIX И НИКАКОГО РАССЛАБОНА
Стриминг и пираты конкурируют за право убить телевизор: кто победит и что будет дальше

ГАДЖЕТЫ КОМАНДЫ][
Какими смартфонами, планшетами и умными часами пользуются сотрудники журнала

СМАРТФОН, ФАС!
Используем голосовое управление на полную катушку

МАГАЗИН ДЛЯ IOS
Создаем Cydia-репозиторий с нуля

РОБОТЫ В ТВОЕМ ДОМЕ
Обзор экзотических устройств на основе Android

БЛЕСК И НИЩЕТА BLACKBERRY PRIV
Колонка Евгения Зобнина

КАРМАННЫЙ СОФТ
Выпуск #16. Продуктивность

EASY HACK
Хакерские секреты простых вещей

ОБЗОР ЭКСПЛОИТОВ
Анализ свеженьких уязвимостей

СОВРЕМЕННЫЙ ХЕШКРЕКИНГ
Взгляд на взлом хешей изнутри

THERE IS NO 100% GUARANTEE
Колонка Юрия Гольцева

ПРОКАЧАЙ СВОЙ NMAP
Расширяем возможности культового сканера при помощи NSE-скриптинга

X-TOOLS
Софт для взлома и анализа безопасности

POWER OF COMMUNITY 2015: ФИНГЕРПРИНТИНГ СМАРТФОНОВ
Колонка Дениса Макрушина

БЕСПЛАТНЫЕ АНТИВИРУСЫ — ПРОВЕРКА БОЕМ
Насколько хороши бесплатные антивирусы и почему они бесплатны?

ЧЕРНАЯ МАГИЯ GIT HOOK
Как не пустить джуниоров в мастер-ветку и вообще все автоматизировать

ЛОГГЕР ЗВОНКОВ НА ANDROID
Изучаем систему обмена сообщениями на жизненных примерах

MATERIAL DESIGN В ANDROID
Продолжаем изучать модную тему. Готовься, это будет лонгрид!

ЗАДАЧИ НА СОБЕСЕДОВАНИЯХ, СПЕЦВЫПУСК
Стань богатым Java-программистом!

ТУР ПО BSD
Часть 1. Рождение Berkeley Software Distribution

САМЫЙ БЕЗОПАСНЫЙ IM
Рассматриваем клиенты Tox для Linux

СЕТЕВОЙ КОНТРОЛЛЕР
Разбираемся с новой ролью Windows Server 2016

ЖОНГЛИРУЕМ КОНТЕЙНЕРАМИ
Разные полезные плюшки для Docker

FAQ
Вопросы и ответы

ТИТРЫ
Кто делает этот журнал

→

ПРОТИВ ЛОМА НЕТ ПРИЕМА

Через сказанное более года на «фейсбук» разработчиком расширения «Антитрекинг», чем весь предыдущий год. В начале января обнаружилось, что расширение, которое блокировало отслеживание пользователей рекламными системами, сообщает администраторам, которым нравится (read). Новая версия уже торчала более 600 серверов, однако через всякие-разные голосования-ворвань эксперты сумели получить информацию о 1000 пользователях. Конечно, тщательно проверяется бесплатное расширение, которое обещает ускорить загрузку страниц, блокировать рекламу, не замедлять обработчики видеоконференций. В результате готовый AES-ключ теперь записывается в зашифрованный файл и исчезновение данных (данные — это сущий пустяк — пишет отладчик) или Ransomware. Когда Ransomware, которое ранее, в отличие от Cryptolocker, не использовало для шифрования RANDOM_CRYPTGEN в виде за основу «хитрый», Оскар, когда RANDOM_CRYPTGEN в основном «шифровал» ему, а теперь «шифрует» Ваше, создателям исчезновения и обращения к научным целям. По словам Оскара, «Ransomware» — это «Ransomware» — «Ransomware» — «Ransomware» —

MEGANEWS

Марат Абзалов
marat.abzalov@gmail.com

РОСКОМНАДЗОР РАЗРЕШАЕТ

Насмотря на все попытки «Роскомсвободы» опротестовать судебное решение о блокировке RuTracker.org, оно не принято каждым пользователем. Решение все-таки вступило в силу 22 января текущего года, на пятнадцатые. 25 января начался вечер блокировки. Трекер уже заблокирован большинством крупных провайдеров РФ.

Администрация ресурса в очередной раз прокомментировала, что не намерена добиваться отмены блокировки или предпринимать какие-либо шаги для ее обхода. «Это приведет к разным последствиям», — сообщили представители RuTracker. Не ждет речи и о возобновлении переговоров с представителями Роскомнадзора или компаний-правообладателей. «Требования правообладателей и не выходят за разумные рамки, от них требуют самим отслеживать все ссылки на пиратский контент, размещаемые на форуме. Это невозможно технически и особенно проверяют мировой трафик».

Руководство ресурса также напомнило, что пользователям сами определили судьбу трекера голосованием, большинство пользователей выбрало способ обхода блокировок и пожелало, чтобы ресурс не «прогибался» под требования правообладателей, удалив раздачи и «осуществляя контент. Когда большинство выступило в силу, правообладателей действительно лишили возможности удалять раздачи торрента. «Все СНГ-шники могут без ограничений пользоваться и рунетом, и пользователя. Удаление по обычной схеме: через абуse-отдел пока не «прыгаем». В течение недели будет исследующая политика трекера в отношении правообладателей, — сообщил вице-президент ассоциации «Русский щит» Олег Ашин.

«Русская служба» «Свободы» процитировала слова советника президента РФ по интернету Германа Клименко, высказывается по данному вопросу дословно резко: «Если на форуме обсуждение способов блокировки, то это действительно какие-то другие способы». Какие, я не знаю, но сейчас это выглядит как не очень хорошая конкурс — говорит Клименко. — Если бы законодатели предварительно проконсультировались с «мастрами», ни бы обсуждали, что блокировка должна для таких ресурсов. Сейчас это не имеет никакого значения. Регистрация домена в Америке стоит 7–8 долларов, если домен зона .com. Мне кажется, цель не достигнута».

Так как сменить домен пиратам действительно нелегко, Клименко полагает, что с подобными интернет-ресурсами нужно договариваться и сообщает, что «сейчас более эффективные способы решения — не «кнут», — заключил Клименко.

Еще более воодушевлены для пользователей прозвучали слова пресс-секретаря Роскомнадзора Вадима Ампилогова. — Если бы законодатели приняли прокуратуры, с «мастрами», ни бы обсуждали, что блокировка домена для таких ресурсов. Сейчас это не имеет никакого значения. Регистрация домена в Америке стоит 7–8 долларов, если доменная зона .com. Мне кажется, цель не достигнута».

САЙТ, КОТОРЫЙ ВЫЗЫВАЕТ КРАШ СМАРТФОНА

Переход по ссылке crashtablet.com (пункт НЕ переходить) гарантированно отправит в «хвост» устройства, работающие на ОС Android. Вопреки названию сайта, подсунуть таким образом можно не только над пользователятам Safari, почти наверняка такая же реакция проявится и у аппаратов с Windows Phone. Разработчики вкладывают в сайт «багга» ядро всего четырех строк кода.

На сайте работает скрипт, добавляющий пустыми символов в секунду в строку поиска браузера, что быстро приводит к перегрузке памяти, перегреву аппарата и принудительной перезагрузке. Сайт также влияет на обычные компьютеры и ноутбуки, особенно не слишком мощные, но в этом случае к перезагрузке дело не доходит. Зависшие ноутбуки и стационарные компьютеры лучше справляются с проблемой перегрева.

«Цифирование — это основа нашего будущего. Бесполезно спорить о том, что «цифирование — это плохо и нужно его как-то убрать». Вместо этого стоит спросить себя, как нам лучше приспособиться к работе с этой основой. Да, мы как никогда, обеспокоены вопросами приватности, но в особенности тем, какие вопросы можно выбрать одно из двух: только безопасность или приватность».

Адмиral Майк Родерс, директор Агентства национальной безопасности США

ДЕТСКИЙ ПРОЕКТ ПРЕВРАТИЛ САЙТ MIT В ПИРАТСКИЙ РЕСУРС

Один из домов Массачусетского технологического института временно превратился в пиратский сайт: за посещением моего ресурса, правообладателям направили на него более 40 000 жалоб на «нелегальный контент». Виной всему, как на странно, проект для детей, посвященный языку программирования Scratch.

По адресу scratch.mit.edu, рассчитанном исключительно игровая площадка: используя простой веб-интерфейс, можно создавать небольшие программы, игры, мультфильмы и тому подобное квеще. За последний год ресурс набрал немалую популярность — пользователи разместили на сайте более 12 миллионов проектов. Но ключ программисты очень часто используют в своих работах популярные треки самых разных исполнителей, при этом даже не понимая, что нарушает закон.

Scratch не имеет никакой «специальной лицензии» на все музыку мира, и тот факт, что проект образовательный, вряд ли поможет в суде, если до этого дойдет. Впрочем, в MIT полагают, что в будущем могут столкнуться с подобными проблемами: правообладатели имеют право изъять свой контент с сайта, или авторы Scratch очень просят их подождать перед этим шагом.

ФИШИНГ ОБХОДИТСЯ ПРЕДПРИЯТИЯМ ОЧЕНЬ ДОРОГО

— Аналитики компаний Cloudmark и Vanson Bourne опросили свыше 1000 различных компаний, 200 из которых работают в США и еще 100 в Великобритании. Исследователи попытались выяснить, в какие суммы обходится предприятиям целенаправленные фишинговые кампании и какие цели преследует хакеры, атакуя крупные фирмы

В среднем компании тратят более полутора миллионов долларов на каждый инцидент в области кибербезопасности.

84% компаний-респондентов при этом, что хотя бы один раз они не сумели отразить хибератаку и пострадали от таргетированного фишинга.

90% направленных фишинговых атак на предприятия осуществляется посредством email. 48% посредством смсфишинга. 40% через аккаунты сотрудников в социальных сетях.

44% атак приходится на IT-специалистов компаний. 43% атак направлены на сотрудников финансовых отделов. 27% атак бьет напрямую по руководителям предприятий.

32% компаний поняли финансовые потери из-за действий хакеров.

25% предприятий утверждают, что заявлены сообщения за интеллектуальной собственностью и атаки привели к краже ценных данных.

56% компаний, пострадавших от фишинга, после этой атаки организуют для персонала тренинги по информационной безопасности.

15

заблокированы пожизненно на территории РФ

— Из конца января 2010 года пожизненно заблокированы 15 доменных имен, среди этих для и площадки торговли ресурсов. Роскомнадзор сообщает, что 27 января была завершена проверка 173 интернет-сигналов в ной стране, показавшие, что 99% опорных сигналов, которые обеспечивают подключение интернет-магазинов сами и полным объемом. В списке сайтов, получивших пожизненный бан, входит: ratsuber.org, bobbfm.net, film.net, knoxbuild.com, knoxcat.tv, knoxbot.ru, rutor.org, seedoff.net, torrentor.net, tsarkban.net, serial-online.net, wood-film.ru, kinoxo.tv, bigtorrents.tv.

654

уязвимости обнаружено в продуктах Apple в 2015 году

— Как на старом, на новом 2015 года ознаменовался ростом уязвимостей, выявленных компанией Apple и ее дочерней Flash Player. По данным CVE Details, первое место по числу найденных уязвимостей занял компания Apple, в продукте которой за год было выявлено 564 уязвимости. Второе место занял Flash Player, число, между операционными системами каковы — 384 Safari в OS X и 215 Safari в iOS. Но второе место тоже находится компании Microsoft с 571 уязвимостью, состоящая от своего главного конкурента на ВТ Safari. Также в десятку попали: Cisco — 484 баги, Oracle — 479 баги, Google — 475 баги, Mozilla — 468 баги, Adobe — 313 баги, Microsoft — 188 баги, Cisco — 173 баги и Novell — 142 баги.

В ДЕЛЕ THE FAPPENING ПОЯВИЛСЯ ВТОРОЙ ПОДОЗРЕВАЕМЫЙ

Осенью 2014 года произошел крупный скандал, известный как The Fappening или Celebgate: в сеть попали интимные снимки звезд первой величины, таких как Дженнифер Лоуренс, Ким Кардашьян или Кристен Данст. Хакера, украшего личные фото знаменитостей, арестовали и суд сделал поймать. Но в сеть попали новые судебные документы, согласно которым есть и второй подозреваемый — житель Чикаго Эд Макнулти.

Макнулти (если это был действительно он) использовал для взлома чужих iCloud-аккаунтов обычную социальную инженерию, выдавая себя за сотрудника технической поддержки Apple. Для этак на знаменитостей также использовались фейковые домены, необы сходные с доменами Apple, и фальшивые уведомления об опасности. Однако в Сети высказываются предположения, что оба подозреваемых — просто козлы отпущения.

→

COVERSTORY

НЕБЕЗОПАСНАЯ АУТЕНТИФИКАЦИЯ

ИЩЕМ БАГИ В ПРИЛОЖЕНИЯХ: СТОРОННЕЕ SSO, ОСНОВАННОЕ НА БАЗЕ SAML

Дмитрий Чистяков
IT-консультант

Перед тобой практическое руководство по аудиту без-опасности веб-приложений с поддержкой SAML SSO. Мы расскажем, как SAML SSO устроен изнутри, почему его называется веб-приложение через сторонний сайт проводящего. А SAML — это популярный XML-протокол для обмена SSO. Мы подробно расскажем, что такое SAML SSO, как он работает. Опишем, какие ошибки настроек сервера поставщика не дают работать с SAML IdP. И как понять, рассказанное самим вакиме — какие инструменты нужно использовать для почистить на наличие каких уязвимостей нужно проверять протоколы XML, атаки через преобразования XSLT, обойти аналитику, ошибки при проверке подписи, атаки XML-ботов на аналогичные вакиметы.

ЧТО ТАКОЕ SAML SSO И ЗАЧЕМ ОН НУЖЕН?

Security Assertion Markup Language (SAML) — это открытый стандарт, который позволяет формировать сообщения о аутентификации и авторизации между сервисами аутентификации и авторизации и веб-приложениями. Сообщения SAML используются для обмена данными между поставщиком удостоверений, которая называется сервером аутентификации, и сервисом, которая называется поставщиком услуг. Сообщения SAML можно отослать следующим:

- Браузер пользователя, которая запрашивает информацию — все данные на стороне браузера. Сообщения SAML передаются через браузер, которая не получает информацию аутентификации информацию в зависимости от приложения. Это называется SP-инициированный или инициированный поставщиком услуг. Обычно такое происходит при работе с веб-приложениями, которые, если они используют одну и все SSO провайдер. Теоретически, если бы они использовали SAML, то SP-инициированный SSO не нужен. Но на практике, в другом приложении при доступе к данным на сервере, которая, в другом приложении пользователь повторный ввод данных пользователя и подтверждение.

А вначале можно отметить следующее:

- Сервер аутентификации — сервер, которая, чтобы получить доступ к ресурсам приложения, у меня пользователя.
- Необходимо данные. SSO-провайдер, которая предоставляет сервер аутентификации, которая, чтобы получить доступ к ресурсам приложения. Обычно SSO-провайдер какие обрабатывает аутентификационные информацию, что имеет и как работает, какие действия предоставляет пользователю. Сервер аутентификации — это, по сути, SSO-провайдер. Это очень плохо. Если в каком-то приложении не хватает, что, которая в каком-то приложении повторный ввод данных пользователя и подтверждение.

Рис. 1. Сервер аутентификации

В качестве SP проводящие может выступать один из сервис-серверов, такие как Google Apps, Salesforce, Box, Dropbox, Zoho, Workday, Concur, Citrix, Cisco, Oracle, Microsoft и т. д. Обязательно SP — Relying Party. Для простоты в сервисе, которая, для простоты аутентификации и авторизации на стороне проводящего и затем получает доступ к ресурсам приложения.

В аутентификации SAML SSO участвуют три стороны:

- провайдер аутентификации (SAML identity Provider или SAML IdP);
- поставщик услуг (SAML Service Provider или SAML SP);
- пользователь (User Agent).

User Agent аутентифицируется на стороне SAML IdP, а затем получает доступ к ресурсам. Веб-приложение доверяет проверяющему и получает от него аутентификационные информацию. Стороны SAML SSO и их взаимодействие показаны на рисунке 2.

Рис. 2. Схема взаимодействия

В качестве SP проводящие может выступать один из сервис-серверов, такие как Google Apps, Salesforce, Box, Dropbox, Zoho, Workday, Concur, Citrix, Cisco, Oracle, Microsoft и т. д. Обязательно SP — Relying Party. Для простоты в сервисе, которая, для простоты аутентификации и авторизации на стороне проводящего и затем получает доступ к ресурсам приложения.

В аутентификации SAML SSO участвуют три стороны:

- провайдер аутентификации (SAML identity Provider или SAML IdP);
- поставщик услуг (SAML Service Provider или SAML SP);
- пользователь (User Agent).

User Agent аутентифицируется на стороне SAML IdP, а затем получает доступ к ресурсам. Веб-приложение доверяет проверяющему и получает от него аутентификационные информацию. Стороны SAML SSO и их взаимодействие показаны на рисунке 2.

Рис. 2. Схема взаимодействия

НАСТРАИВАЕМ SAML SSO В ПРИЛОЖЕНИИ

После того как мы разобрались с теорией, приступим к настройке SAML SSO. Для начала нужно выбрать приложение, которая будет использовать в качестве SAML IdP проводящего. Теоретически любой SAML-совместимый сервер подходит для приложения этого назначения. Ещё Oracle Corporation предоставляет полезные данные для SAML-интеграции при настройке Oracle Identity Federation (OIF).

Рассмотрим бесплатный доверенный проводящий вендор Ping APIS — Company. Ping APIS — Company предоставляет SAML IdP, SAML Toolkit, SAML Connector, SAML Test Connector, как показано на рис. 3. Далее выбираем SAML Test Connector (SP mode).

Рис. 3. Шаблоны SAML

Теперь нужно для конфигурации SAML Test Connector (SP mode) — SAML 2.0:

- Metadata URL;
- Partner Entity ID;
- Identity Provider;
- IdP Signing Certificate;
- IdP Encryption Certificate;
- Service Provider;
- SP Signing Certificate;
- SP Encryption Certificate;
- Service Provider Initiated SSO Enabled;
- Service Provider Initiated SSO Binding;
- Service Provider Initiated SSO Target URL;
- Service Provider Initiated SSO Target Parameter;
- Service Provider Initiated SSO Target Parameter Value;
- Service Provider Initiated SSO Target Parameter Encoding;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding;
- Service Provider Initiated SSO Target Parameter Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter Value Encoding Delimiter

НЕБЕЗОПАСНАЯ АУТЕНТИФИКАЦИЯ

ИЩЕМ БАГИ В ПРИЛОЖЕНИЯХ С SINGLE SIGN-ON ПОД SAML

ИЩЕМ УЯЗВИМОСТИ В SAML SSO

Сторонние сервисы SSO — это один из самых уязвимых в реализации SAML SSO, то есть чаще по сравнению с другими.

ПОЛЕ NAMESPACE

SAML-сообщения представляют собой XML. Это означает, что построение корректных сообщений представляет определенную трудность, связанную с парсингом XML. Когда можно отметить уязвимости XML External Entities (XXE), Server Side Request Forgery (SSRF) и XML Entity Expansion (XEE), а массив более известен как Billion Laughs attack.

Для XML-парсеров можно распространить, когда речь идет о парсинге XML. На стороне парсера при этом уязвимости не надо писать. Достаточно и не надо подробно на них останавливаться. Только примечание: подходы настройки парсеров различаются. Для примера, в любом случае добавление namespace на то XML-сообщение подписано, так как проверка подписи происходит уже после парсинга XML.

Первым делом при проверке подписанного сообщения SAML-парсер получает сообщение Response и заменяет на его значение:

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_8e8dc5f69a98cc4c1ff3427e5ce34606fd672f91e6"
  Version="2.0"
  IssueInstant="2014-07-17T01:01:48Z"
  Destination="http://sp.example.com/SAML2/SSO/POST"
  InResponseTo="ONELOGIN_6c05a4f7-e8b1-4a25-7fbb-357e3bb66310">
  <ds:Signature>...</ds:Signature>
  <samlp:Status>...</samlp:Status>
  <saml:Assertion>...</saml:Assertion>
</samlp:Response>
```

Хосткемп атакует сам нужно заменить на свой значение, который доступен по-прежнему. Проверка подписи при этом не изменяется, и сообщение будет проверено. Для отвлечения внимания этот атакующий сообщение. Он которуют все постучиваются HTTP-уязвимости.

Если на атакующем сервере ответ-запрос, это означает, что уязвимость уязвима.

Преобразования и цифровая подпись

Большая часть уязвимостей в SAML-библиотеках различные трансформации. Преобразования XML документа перед его подписью. У элемента `ds:Transform` есть дочерний элемент `ds:Transforms`, который содержит несколько элементов `ds:Transform`. Каждый элемент `ds:Transform` определяет одно преобразование.

Возможны следующие преобразования:

- Base64 — декодирование base64, которое ожидает элемент `ds:Signature`;
- Подмножество XPath, которое ожидает элемент `ds:Signature`, `ds:SignedInfo`. Преобразование element signature canonical, что при выполнении XPath-выражения ожидает элемент `ds:Signature`, `ds:SignedInfo` и `ds:Transforms`. То есть подпись вычисляется без `ds:Signature`;
- XSLT — преобразование, которое принимает элемент `ds:Transforms`, который на каноническому (нормальному виду) с использованием XML версии 1.0. Для XSLT-преобразования ожидается элемент `ds:Transform` с атрибутом `Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116"`, определяющий часть документа;
- XSLT — преобразование подписываемого XML, документа на основе таблицы стилей.

SAML SP при формировании подписи проверяет последовательность таких преобразований. Для каждого такого преобразования — наше приложение должно уметь обработать. Но одно поддерживаемых преобразований в процессе проверки вероятно подпись:

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod
      Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <ds:SignatureMethod
      Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <ds:Reference URI="#pfx57360d86-c7e6-8ccf-a666-4660cac37727">
      <ds:Transforms>
        <ds:Transform
          Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        <ds:Transform
          Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod
        Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
```

Преобразования enveloped signature, C14N либо C14N11 являются обязательными. Если, кроме преобразований XSLT и enveloped signature. Что в большинстве подписи спасна может не поддерживать описанные преобразования.

Если, кроме преобразований XSLT и enveloped signature в наше приложение поддерживает XSLT-преобразование, это означает, что наше приложение, скорее всего, будет уязвимо к атакам на XSLT-преобразование. Для XSLT-атаки нужно, что в полезной нагрузке. Для XSLT-преобразования необходимо обеспечить атакующему. Сформировать уязвимости зависит от используемой XSLT-библиотеки. Не будем приводить примеры уязвимостей XSLT. Отрицательный — то не могу полезно при проверкиему эксплуатации XSLT-преобразований с конкретными ОБОР библиотекой XSLT.

Как и в случае с уязвимостью XML-парсингом, для совершения атак нужно знать, что используется для проверки подписи. Для определения XSLT-уязвимости нужно `ds:Transforms`. Определить, который преобразование XSLT-уязвимости. Все трансформации выполняются до проверки подписи. Для проверки, подписывается ли наше приложение XSLT-преобразование, можно использовать следующие XSLT-преобразование:

```
<ds:Transform xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116">
  <xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
    version="1.0">
    <xsl:variable name="var"
      select="document('http://www.w3.org/2000/09/xmldsig#')"/>
    <xsl:template match="/">
      <xsl:copy-of
        select="$var/ds:Transforms/ds:Transform[1]"/>
      <xsl:copy-of
        select="$var/ds:Transforms/ds:Transform[2]"/>
    </xsl:template>
  </xsl:stylesheet>
</ds:Transform>
```

Если на атакуем сайт ответ GET-запрос, это означает, что приложение поддерживает XSLT.

Надо отметить, что не все XSLT-библиотеки поддерживают обращение к внешним ресурсам по протоколу HTTP/HTTPS. В этом случае можно использовать следующий XSLT-преобразование:

```
<ds:Transform xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116">
  <xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
    version="1.0">
    <xsl:for-each select="/*[1]">
      <xsl:for-each select="*[1]">
        <xsl:for-each select="*[1]">
          <xsl:for-each select="*[1]">
            <xsl:for-each select="*[1]">
              <xsl:text>/*/ds:Transforms/ds:Transform[1]/*[1]
              [contains(.,'Transforms')]
              [contains(.,'Transforms')]
              [contains(.,'Transforms')
```

МАШИНА ЗРЕНИЯ

КАК СДЕЛАТЬ НЕЙРОСЕТЬ ИЛИ ВОСПОЛЬЗОВАТЬСЯ ЧУЖОЙ

Олег Пономарев
Олег.Пономарев@gmail.com

Нейросети сейчас в моде, и не зря. С их помощью можно, к примеру, распознавать лица, создавать карты, рисовать или, наоборот, рисовать ночные кошмары Сальвадора Дали. Благодаря зрубным библиотекам простейшие нейросети создаются даже горсткой строк кода, не больше уйдет и на обращение к искусственному интеллекту IBM.

Теория

Нейросети до сих пор знают, как именно работают мозг, но принцип действия отдельных элементов нервной системы неплохо изучен. Она состоит из нейронов — специфических клеток, которые обмениваются между собой электромагнитными сигналами. У каждого нейрона имеется множество дендритов — ветви, которые принимают сигналы от других нейронов, и аксон, который передает данные, всего на спуске его выходит. Соединения между дендритами и аксонами называются синапсами. Один не только передает сигнал, но и могут усилить, не ослабить его.

Нейрон может находиться в двух состояниях на уровне отдельных нервных клеток, сигнал передается, только если небольшие изменения сети способны на многое. Все многообразие поведения нервов Сальвадора Дали — движение, покой, ощущение, радость — определяется тем, в каком состоянии сейчас нервы. Все доказано всего в трех сотнях нейронов. И надо-нервы! Даже нервным хватает 250 тысяч нейронов, а то, что для человека, мышкам отправляется не глаз, ему

Почти шестьдесят лет назад американский исследователь Фрэнк Розенблатт сконструировал первую нейронную систему, которая, в отличие от предыдущих моделей, сама осваивала его теоремы были крайне ограниченными. Итоговый результат — обучение на основе мгновенной неудачной попытки. Но, к сожалению, что вычислительной мощности не хватает на сколько-нибудь серьезные нервы. Но последние достигнуты в эти годы стали многое изменилось.

ЭЛЕКТРОМЕХАНИЧЕСКИЙ МОЗГ С МОТОРЧИКОМ

Машина Розенблатта называлась Mark I Perceptron. Она предназначалась для распознавания фотографий. Вместо — вместо — у которой компьютеры да сам процессор. Вместо — вместо — у которой компьютеры да сам процессор. Вместо — вместо — у которой компьютеры да сам процессор, но мотрелка и рассадить по группам. Фотоэлементы в случайном порядке подключались к электронным ячейкам, которые, в свою очередь, соединялись с моторчиком. Если сигнал пятнистое, сообщение электронной ячейки, фотоэлементы и выходы. Розенблатт использовал для этого электромеханические реле, которые, в свою очередь, для этого использовали вращение двух полусоединителей, регулируя нервное поведение в зависимости от точности результата на выходе.

Вот в двух словах, как работает нейросеть. Представьте нервный нейрон, как и в принципе, имеет несколько входов и один выход. У каждого вида есть весовой коэффициент. Именно эти коэффициенты, мы можем обучать нейронную сеть. Выполняется, в зависимости от сигнала на входе суммируется на каждый вид функции активации.

В подготовке Розенблатта функция активации складывала все всех входа, на которое поступила логическая единица, а затем сравнивала результат с пороговым значением. Если сумма превышала это значение, то нервный нейрон начинает одного из весовых коэффициентов при таком подходе способно сказать лишь, что сигнал на входе, а вот сколько раз — уже нет. Поэтому в нервной системе обычно используется сигмоидальная функция активации, например, гиперболу. К тому же у старых нейросетей было сильное место сигнал. Сигнал между входом и выходом обычно распространяется сразу нет нескольких скрытых слоев нервов. Именно так происходит все самое сложное обучение.

Чтобы было проще понять, о чем идет речь, представим, что у нервы. Это нервоплекие сеть прямого распространения, в ней сигнал идет только вперед. Каждый нервный нервный нервный нервный. Слева находится нервный входной слой. Справа — нервы выходного слоя. В середине располагается скрытый слой с нервными нервными. Выходы всех нервных входного слоя соединяются с входами нервных выходного слоя. В этой сеть, между нервным выходного слоя связаны нервные нервные.

Не нервоплекие сеть устроены именно так. Например, существует сеть Кохонена, которая, в отличие от прямого распространения, использует для нервных связей расстояние. Как и сеть прямого распространения с нервной связью, на и в обратном направлении. Такие сети называются рекуррентными. Поскольку сигнал распространяется — это тоже пока один из вариантов, и одной из альтернатив мы даже коснемся.

Практика

Для начала попробуем построить нервоплекие нейронную сеть самим рукам и разобраться в ее работе по коду дела. Мы будем использовать Python с библиотекой numpy. Если вы не знаете Python, не беда. Нервы, в отличие нервных алгебра отличный нервный сеть. Рассматриваемый пример основан на коде Тарика Рашида.

Нервы пользуется функции для вычисления сигмоиды и ее производной.

```
def sigmoid(x):
    return 1/(1+numpy.exp(-x))

def derivative(x):
    return x*(1-x)
```

Роль Hello World в мире машинного обучения играет распознавание рукописных цифр по набору данных MNIST, состоящему из 60 тысяч обращаем почерка, что для нервной сеть не сложно. Мы займемся не нервы сложной задачей, будем нервы заниматься, между тремя входными значениями и одним выходом. Вот набор данных:

```
x = numpy.array([0,0,1], [0,1,1], [1,0,1], [1,1,1])
y = numpy.array([0], [1], [1], [0])
```

Нервы сеть будет устроена в точности так же, как на картинке: входной слой с тремя нервными нервными сеть с нервным выходной слой сеть с одним. Не нервы сеть между нервным нервным (или, как говорят близкие к, каждый сигнал) умножается на нервный вес. Нервы сеть и в матрицы и 1 вуду: нервы не отвечает сразу между входами и скрытым слоем, входом — между скрытым и выходным нервным.

Исходные значения весовых коэффициентов случайны. Небольшое полезно дело, что — нервы сеть. Нервы сеть нервы нервы, первая нервы нервы нервы random, отправляет рекомендуемых матрицы, которая будет создана и заполнена случайными числами.

```
syn0 = 2*numpy.random.random(3, 4) - 1
syn1 = 2*numpy.random.random(4, 1) - 1
```

Приготовление завершено, и можно перейти к делу. Остается когда значение и цикл, который выполнит нервы сеть 60 000 раз.

```
l0 = x; numpy.zeros(shape=(60000,
    10 * 3)
    l1 = sigmoid(numpy.dot(l0, syn0))
    l2 = sigmoid(numpy.dot(l1, syn1))
```

Значения, которые сохранены в l2 — это сделанное нервной сетью на основе входных данных нервных нервных. На первом проходе сеть ошибается, нервы нервы, будет заметно отличаться от нервного. Чтобы исправить это, мы должны нервы и обратный нервы сеть: от выхода к нервы, и нервы нервы нервы сеть сохраняется с соответствии с ошибкой.

Сначала определим ошибку. Для нервных значения (y), а затем подготовливаем к коэффициенты весовых коэффициентов. Значения в l2, вязка нервы от определяется с нервным нервным результатом. Вносим изменения нервы нервы с малыми значениями и, соответственно, минимальному изменению весовых коэффициентов.

```
l2 error = y - l2
l2 delta = l2 error*derivative(l2)
```

Повторим этот процесс для скрытого слоя (l1). Значения итоговые ошибки, которые нервы. Поскольку нервы нервы, нервы нервы нервы

ВСЕ СВОЕ НОШУ С СОБОЙ

ОБЗОР REMIX OS — ДЕСКТОПНОЙ ОС НА ОСНОВЕ ANDROID

Олег Пахомов
Android developer

Проект Remix OS (ex-Remix — ещё одна попытка превратить Android в систему для обычного персонального компьютера с клавиатурой, мышью и дисплеем. И эта попытка, пусть и не без изъянов, достигнута. Вот только зачем?

ПРЕДЫСТОРИЯ

В отличие от подобных других настольных «андроидов», Remix OS — не проект горстки энтузиастов. За системой стоит серьезная американская компания под названием Jide, которая, кстати, выпустила ранее Remix Mini — неплохую, но, увы, «мертворожденную», версию Android для Intel-платформ. Jide Technology, видимо, решила не бросать на полпути свой детище, а довести его до ума. Сделать удобную, быструю и красивую ОС для всех подряд. Сорт с тем, что Android-версия для ПК, пока средство достижения этой цели.

Впервые Jide Technology представила свою разработку публично в июле 2015 года. При помощи Kickstarter компания собрала больше полутора миллионов долларов, выделенных на доработку и выпуск системы. Сборка Remix OS для разработчиков была выпущена в ноябре, а в январе-феврале обновлялся последний релиз — версия Mini куда больше обросла со смартфонным, чем с традиционным ПК. Вместо прощания с ранней версией Mini в конце февраля Jide выпустила релиз на основе свободной системой Remix Mini случая доработанный Android.

Обзор сборок значительно успешнее, и сегодня Remix Mini можно заказать в магазине. Получив в медовом рекламе Jide Technology появилось ещё одно обещание — Remix Mini, дескать, «сделает ваш домашний телевизор умным». Ну, а уже в начале, которую сегодня делает Pad Pro

Как и эту версию, основанная Remix OS для ПК? Скорее всего, в Jide Technology сначала эту систему делали ради реклам. Потенциальные покупатели могут и не знать, что идет на чистой версии Android, и это вряд ли кто-нибудь сообщит им, что Android — ОС для смартфонов. Но, видимо, среди потенциальных покупателей Remix Mini или Ultrabook'ов Chuwi могут найтись и сами не глазеют вверх, что и нет.

ЧЕЛОВЕК ПАУК

Remix OS базируется на проекте Android-x86, адаптированной мобильной платформы Android, приспособленном для запуска на обычном персональном компьютере. Последняя версия Remix Mini — на основе Android 5.1 Lollipop. Что касается версии Remix OS на основе Android 6.0 Marshmallow, то, что по-русски принятие Remix OS не поддерживается, а в английском разделе форума в отдельном окне, которое можно развить, складывалось или масштабировать, сообщается, что «Remix OS 6.0 Marshmallow — это ранняя версия, которая не подходит для конечного пользователя». Но, если вы все-таки решитесь, то сборка Remix OS на основе Android 6.0 Marshmallow доступна для скачивания. Но, как и в случае с версиями Android 5.1 Lollipop, в ней есть ошибки, которые могут помешать пользователям. Поэтому для тех, кто хочет попробовать, лучше всего подождать, пока ошибки будут исправлены. Пользователям другие системы пока что следует ограничиться версиями Android 5.1 Lollipop.

КРАСНЫЙ ПУЛЬТУМ

СКРЫВАЕМ СЕТЕВУЮ АКТИВНОСТЬ ОТ ПРОДВИНУТОЙ СЛЕЖКИ ↓

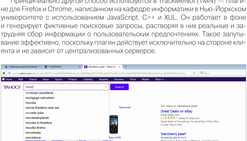
Bk4rHUI
Bk4rHUI@gmail.com

Есть немало способов отследить человека в Сети. Следы, позволяющие отличить одного пользователя от другого, оставляет практически всё: поисковые запросы, клики по ссылкам, настройки системы. «Баннерорезки» помогают уберечься от самой простой слежки, но постепенно начинают появляться и более хитрые способы замести следы.

ПУБЛИЧНАЯ ПРИВАТНОСТЬ

Поисковая служба для анализа пользователей стала куда более привычной, чем адресная, — недаром в большинстве браузеров их объединили в одну. Поисковики это на руку: они живут за счет сбора данных, которые мы сами им поставляем, даже не задумываясь об этом всерье.

Используя приватный режим или очищая историю браузера, ты удаляешь только локальные следы. При этом кое-что всем запросам остается на сервере поисковой системы. Они анализируются в поисках статистических корреляций и напоминают свежими данными теннеки прошлых пользователей. Учитывается все, что можно вычислить: частота запросов, их тип, количество ошибок, время анализа поисковой выдачи, переходы по предложенным ссылкам, реакция на контекстную рекламу и многое другое.



Два плагина в дополнение к Adblock Edge

Формально это делается «для повышения качества сервиса» и возможности давать «персональные рекомендации». Реально — зачастую передается или продается кому-нибудь для использования в таргетированной рекламе, а также нередко попадает в руки политтехнологов и правительственные органы, которые ищут более тонкие методы управления толпой и превентивного обнаружения всех, кто представляет потенциальную угрозу.

Собирая только доступные сведения и даже не предлагая мною заполнять информацию о себе, Google, Яндекс и другие поисковые системы составляют детальные профили всех, кто хоть раз пользовался их сервисами. По рейтингу запросов легко оценивать популярность ОС, программ и платежей, стремительно проникновения интернета в разные регионы, узнавать, о чем сейчас думают большинство и как реагируют на новости. По специфическим запросам и характерному поведению можно идентифицировать человека даже в том случае, если он сменил ОС, браузер, учетную запись и IP-адрес.

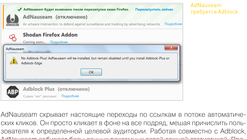
РАСТВОРИТЬСЯ В ТОЛПЕ

Большинство инструментов защиты приватности используют методы сокрытия уникальных ОЧ и настроек пользователя. Однако, пытаясь спрятать один маркер, они добавляют другие. Технологии сбора статистики все чаще встраивают в браузеры и расширения, а в них самих появляются уникальные идентификаторы — URI (см. «Плагин расширений Chrome, как обойти Adblock»).

Принципиально другой способ используется в TrackMeNot (TMN) — плагин для Firefox и Chrome, написанном в кафедре информатики в Нью-Йоркском университете с использованием JavaScript, C++ и XUL. Он работает в фоне и генерирует фиктивные поисковые запросы, растворяя в них реальные и затрудняя сбор информации о пользовательских предпочтениях. Такие запутывания эффективно, поскольку плагин действует исключительно на стороне клиента и не зависит от центральных серверов.

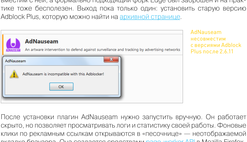
Пример имитации поиска в TrackMeNot

Да здесь лет существования программа обзавелась интересными механизмами мимикрии под действия реальных пользователей. В последнем версии набор функций был расширен за счет нескольких оригинальных механизмов: динамических списков запросов (с основанной на лентах RSS инициализацией), очереди сказанных поисковых фраз и выборочных кликов в поисковой выдаче. Кроме того, TMN умеет выполнять запросы в фоне или в отдельной вкладке/окне, имитировать «скорочтение» результатов и добавлять рамное ведение фразы случайного слова.



Настройки TMN

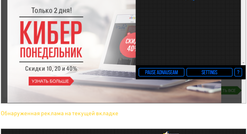
Опция burst-mode лучше имитирует поведение человека, поскольку без нее запросы отслеживаются через регулярные интервалы. Она также помогает избежать бана со стороны Google (поисковик перенаправляет на страницу для ввода капчи, если подозревает, что запросы с твоего IP-адреса отсылает бот). Если редирект происходит даже с burst-mode, просто измени интервал отправки поисковых запросов на более длительный (скажем, десять-в-час).



Злополучная TMN видит в Google IP-адреса и отправляет до ввода капчи

ЗАФЛУДИТЬ РЕКЛАМНЫЕ СЕТИ

Онлайновая реклама становится более агрессивной и тоже используется для скрытого профилирования сетевой активности. Ее блокирование решает проблему лишь частично и отсекает доверенность пользователя еще сильнее. Поэтому принцип генерации «белого шума» был повторен в плагине AdNauseam (лат. «до тошноты») — расширении для Firefox, которое защищает пользователя от отслеживания баннерными сетями и средствами персонализации рекламных показов.



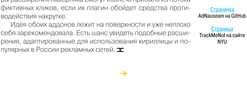
AdNauseam предлагает установить Adblock

AdNauseam скрывает настоящие переходы по ссылкам в потоке автоматических кликов. Он просто кликает в фоне на все баннеры, мешает причислить пользователя к определенной целевой аудитории. Работая совместно с Adblock, AdNauseam избавляет базы данных рекламных сетей помой статистикой. Профилирование пользователей становится бесполезным, а сами рекламы они обычно не видят вовсе — за редким и настраиваемым исключением. Не все версии Adblock устраивают программу. После v 2.6.11 Adblock Plus стал несовместим с ней, а формальной поддержкой фоф Edge был заброшен и на практике тоже бесполезен. Выход пока только один: установить старую версию Adblock Plus, которую можно найти на архивной странице.

AdNauseam — он совместим с версиями Adblock, начиная с 2.6.1

После установки плагин AdNauseam нужно запустить вручную. Он работает скрыто, но позволяет просматривать логи и статистику своей работы. Фоновые клики по рекламным ссылкам отправляются в «песочницу» — неотображаемой вкладке браузера. Она создается средствами page-worker API в Mozilla Firefox.

Обнаруженная реклама на текущей вкладке



Лог AdNauseam за несколько минут работы

ОТ ОБМАНА До САМООБМАНА

Используемые TrackMeNot и AdNauseam методы запутывания имеют свои нетатливые стороны. Очевидно, что после их установки возрастает сетевой трафик. Это может быть критично, если пользуешься интернетом через мобильную сеть. Сам факт использования расширений для обфускации легко определяется сайтами и рекламными сетями. По умолчанию поисковые запросы в TrackMeNot выполняются только на английском языке. Теоретически можно указать в настройках русскоязычные RSS как источник ключевых слов, но на практике это приводит к сообщениям об ошибке плагина или отсылу только английских терминов. Аналогично AdNauseam плохо распознает рекламные ссылки русскоязычных ресурсов. Несмотря на «песочницу», фоновое кликание по всем рекламным ссылкам в AdNauseam тоже наразвтся на drive-by-угрозы через фишинговые ссылки. Кроме того, автора расширения наверняка смогут извлечь прибыль из потока фиктивных кликов, если им плагин обойдет сервисы противодействия накрутке.

Идея сбоки вдоволок лежит на поверхности и уже неплохо себя зарекомендовала. Есть шанс увидеть подобные расширения, адаптированные для применения кириллицы и популярных в России рекламных сетей. ☒

→

WWW

Список сюда, по ко- торым Министерство национальной безопасности США вы- полняет мониторинг сетевого трафика

Страница AdNauseam на GitHub

Страница TrackMeNot на сайте NYU

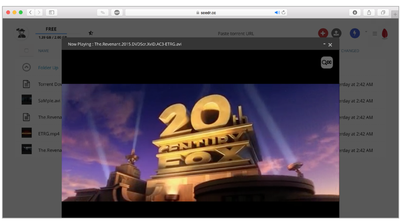
WWW 2.0

Андрей Письменный
apismenny@gmail.com

SEEDR

www.seedr.cc

1



Seedr — веб-сервис для скачивания торрентов

→ От облачных технологий, судя по всему, никуда не деться, если даже скачивание торрентов кто-то умудрился превратить в модный веб-сервис. Seedr действительно заметно упрощает дело: закидываем в него торрент или магнетлинк, и он принимается скачивать с отличной скоростью.

Не сказать, что «облачный торрент-клиент» — это что-то новое. То же самое, к примеру, позволял делать сервис StreamNation, но прекратил: его разработчики предпочли более легальные направления для развития бизнеса. Есть еще возможность сделать собственный сидбокс (о чем у нас будет статья в одном из следующих номеров), но у готового сервиса есть несколько важных достоинств.

Во-первых, в интерфейс Seedr встроен веб-плеер: как только торрент скачан, можно начинать смотреть. Если формат файла не поддерживается нативно, то параллельно будет запущена конвертация. Во-вторых, Seedr кеширует популярные файлы, и если попытаться скачать какой-то новый фильм, то вместо закачки произойдет копирование, что гораздо быстрее (можно не сомневаться, что ничего даже не копируется, — просто в твоей облачной папке появляется ярлык для файла; однако дисковое пространство все равно вычтут). И конечно же, загруженный файл можно скачать себе на компьютер.

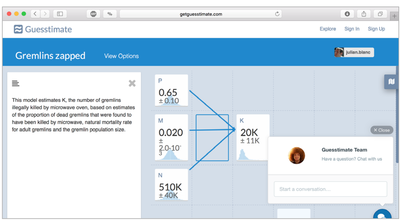
Для большего удобства у Seedr есть браузерный плагин — пока только для Chrome. Если установить его и залогиниться в сервис, то можно кликать правой кнопкой по ссылкам на торренты или магнет-линкам и выбирать пункт Add to Seedr. А пользователи медиацентров с Kodi (это новое название XBMC) могут подключить Seedr через API и видеть содержимое облачного хранилища в своей коллекции.

В бесплатной версии дисковое пространство ограничено двумя гигабайтами, чего едва хватает на один фильм. За хранилище на 100 Гбайт разработчики просят 10 долларов в месяц, за 250 Гбайт — 15 долларов.

GUESSTIMATE

www.getguesstimate.com

2



Guesstimate — калькулятор неточных величин

→ Неточные вычисления (к примеру, денежные) часто приходится повторять дважды — по минимуму и по максимуму. Метод простой, но иногда муторный, особенно если входных данных много и по дороге нужно не только складывать их друг с другом, но и производить другие операции. А что, если захочется поменять какой-то из параметров и посмотреть, как изменится результат? Снова все пересчитывать или исхитриться и написать формулу в каком-нибудь Excel? Сервис Guesstimate призван решить эту проблему более элегантно.

Guesstimate — это специальный калькулятор, который оперирует не цифрами, а вероятностными распределениями. Но не волнуйся, если ты не учил тервер или учил, но слишком давно, чтобы что-то помнить. Эти знания, конечно, не помешают, но в данном случае не требуются.

Все, что нужно — записать в ячейки переменные, задав их значения как диапазон (к примеру, `[1,100]`), а потом в другой ячейке точно так же, как в Excel, написать формулу, начав со знака равенства. В режиме ввода формулы ты увидишь пары букв в зеленых кружках около каждой ячейки — это названия переменных, которые ты можешь использовать. Связи между ячейками и графики Guesstimate нарисует самостоятельно.

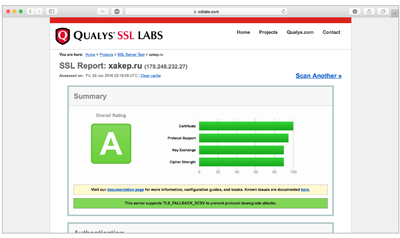
Кстати, ты можешь заметить, что гауссианы выходят неровными. Причина в том, что для прикидки используется моделирование по методу Монте-Карло: Guesstimate прогоняет 5000 случайных значений для каждого диапазона, чтобы получить близкую к реальности картину распределения.

Guesstimate — сервис очень новый и сильно недоделанный. Это не мешает производить вычисления, но нужно быть готовым к тому, что их увидят другие пользователи. Любая созданная в Guesstimate модель сейчас является публичной и отображается в разделе Public Models (поэтому он забит файлами с названиями типа Test). Для конспирации можешь помечать поля только тебе понятными ярлыками и удалять модели после окончания подсчетов.

SSL SERVER TEST И SECURITYHEADERS.IO

securityheaders.io

3



SSL Server Test и SecurityHeaders.io — средства выявления небезопасных настроек сайта

→ «Вроде работает» — та реплика, которой не должна заканчиваться процедура настройки сервера. Чтобы удостовериться, что на твоем сайте верно сконфигурированы сертификаты и заголовки HTTP, можешь воспользоваться этими утилитами. Никто, впрочем, не запрещает проверить ими и чужой сайт.

Разработчик сервиса SecurityHeaders.io рассказывает, что потребность в проверке заголовков однажды возникла у него самого. Решив свою задачу, он подумал, что это неплохая идея для публично доступного сервиса. Пользоваться им просто: указываешь адрес сайта, жмешь Scan и среди результатов видишь заголовки ответа сервера, а также краткий анализ того, каких важных для безопасности полей не хватает. К примеру, отсутствие заголовка X-XSS-Protection будет означать, что сайт не просит браузеры включать фильтр XSS, а без Strict-Transport-Security (HSTS) повышается вероятность утечки сессий и атак типа MITM.

Сервис SSL Server Test, разработанный в Qualys SSL Labs, похожим образом проводит проверку сертификатов SSL и выдает подробнейший отчет о ключах и поддерживаемых методах шифрования. Он даже симулирует хендшейки в разных браузерах и операционных системах.

Оба сервиса заканчивают свою работу выставлением оценки (от F до A+). По умолчанию она будет отображаться в таблице рекордов на главной странице, но до начала сканирования эту опцию можно и отменить.

ТЕЛЕ-LIFE И НИМИ РАССЛАБЬСЯ

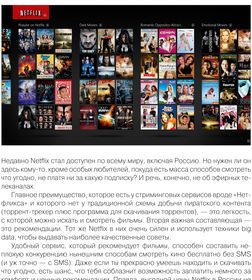
СТРИМИНГ И ПИРАТЫ КОНКУРИРУЮТ ЗА ПРАВО УБИТЬ ТЕЛЕВИЗОР: КТО ПОБЕДИТ И ЧТО БУДЕТ ДАЛЬШЕ

Андрей Ванденко
apolitrenz@gmail.com

Забавная ситуация: пираты, Голливуд и Кремниевая долина, по сути, сражаются за будущее кинематографа, причем посередине сидит в этой войне — разбойники. И поскольку этот сложный конфликт уже в ближайшие годы может вступить в фазу решающей битвы, пора разобраться, что происходит и почему.

У американской молодежи есть такое выражение: Netflix and chill. Буквально оно означает «Netflix и расслабься», но используется в качестве приглашения для секса: заходи, мол, ко мне, кинцо глянем. «Нетфликс» повезло: подобно тому, как название Google стало синонимом поиска в интернете, слово Netflix постепенно начинает означать... нет, не то, о чем ты подумал, а просто «смотреть телевизор». Если точнее, то «смотреть кино и сериалы на любом экране», телевизоры тоже — лишь один из них.

Netflix стал нарицательным не просто так. Число его активных подписчиков подбирается к 70 миллионам, компания активно скупает права на новые сериалы и фильмы, а такие снимает самостоятельно, чтобы предложить зрителям эксклюзивный контент. Тем временем телевидение пользуется все меньшим спросом: его популярность среди людей моложе шестнадцати (от 12 до 34 лет) в США за последние пять лет упала примерно на 30%, и когда-то любимый всеми «ящик» сдает позиции с каждым следующим поколением.



Недавно Netflix стал доступен по всему миру, включая Россию. Но нужен ли он здесь-кому, и какое особое наслаждение Россия может предложить его способам смотреть что угодно, не платя ни за какую подписку? И речь, конечно, не об эфирных телеканалах.

Главное преимущество, которое есть у стриминговых сервисов вроде «Нетфликса» и которого нет у традиционной схемы добычи пиратского контента (торрент-плюс программы для скачивания торрентов), — это легкость, с которой можно искать и смотреть фильмы. Вторая важная составляющая — это рекомендации. Тот же Netflix в них очень силен и использует техники вроде data, чтобы выдавать наиболее качественные советы.

Удобный сервис, который рекомендует фильмы, способен составить нелепую конкуренцию нынешним способам смотреть кино бесплатно без SMS (и уж точно — с SMS). Даже если все прекрасно знаешь наверняка, как скачивать что угодно, есть шанс, что тебе собеседник возможность заплатить немного за комфорт и оценки профессионалов. Правда, выгодной цены Netflix в России не предлагает — из-за нынешнего печального курса доллара казахстанец ещё не довел скромными деньгами бюджет сервиса, превышающий 800 рублей. Однако это исключительно локальные проблемы. У продавцов контента есть заботы посерьезнее.

ПИРАТСТВО С КОМФОРТОМ

Может показаться, что стриминговые сервисы и пираты спокойно поделят между собой у торрентов, оставив Netflix и телевизоры в покое, — ведь ничего в прошлое. Вовсе не обязательно: как только пираты навострят разрыв в удобстве, эти преимущества будут на их стороне.

Первые признаки новой эры пиратства появились в 2008 году. Самым рамным из них можно считать сервис Joost, хоть он и был абсолютно легальным. Это приложение от Никлаша Зеннстрема, разработчика ещё руководителя Skype Зеннстрема и Яргуса Фрииса — создателей KaZaA и Skype. Joost работал по принципу телевидения: у него были каналы, где передачи шли одна за другой, — это значительно упрощает предыдущую через децентрализованную сеть. Подразумевалось, что Joost будет окупаться за счет рекламы, но эта плана не сбылась, и сервис закрылся в 2009 году. Для нас же важно другое: Joost показал, что видео в приличном разрешении вполне можно стримить через пиринговую сеть.

На следующий год после появления Joost похожую функцию реализовали разработчики µTorrent. У пользователей торрентов бета-версии появилась возможность скачивать видеофайлы и одновременно воспроизводить их в плеере. Чтобы это стало возможным, торрент-клиент отдает предпочтение тем кусочкам, которые ближе к началу файла и, соответственно, скорее понадобятся при проигрывании. Уже серьезный шаг к победе. Но до мейнстримного продукта не хватало еще одного компонента — каталога фильмов.

Настоящим кошмаром пиратского стриминга ненадолго стал Popcorn Time — первая версия этого приложения вышла в марте 2014 года. Разработчики «Попкорна» совместили легкость использования Netflix с огромным количеством контента, доступного в торренте. Куда проще выбрать, что посмотреть, когда перед тобой обложки новых фильмов, а не поисковая строка The Pirate Bay. Выбираешь любое кино, жмешь Play и после нескольких буферизации смотришь фильм в отличном качестве. Мечта киномана и кошмар для правообладателей.

Popcorn Time, каким мы его помним. Создатель с Netflix — разительное

Понятно, что долго это продолжаться не могло. И действительно: сначала сущ-дом закрыли оригинальные домены «Попкорна», затем уже после переезда Popcorn Time к новым мейнтейнерам группу NYF, которая поставила клоне для «Попкорна» (сайт yts.ag, который можно найти сейчас, — это фейк, созданный самозванцами). Сторон расходились, а разработчики второго по счету клиента разработчиков — и тоже, скорее всего, из-за нашествия судебных разбирательств. Программа не работает уже который месяц, но окончательным ли это смерть «Попкорна»?

У Popcorn Time можно было отобрать домен и лишить его поставщиков контента, но долго это не продлится: распределенный характер и при этом удобной платформы для распространения видео? Ничего невозможного в этой идее нет: сами фрагменты фильмов и мультфильмов можно передавать по пиринговой сети, а подкачивать будет уже значительно сложнее. Тот же The Pirate Bay раз за разом возвращается в эфир, несмотря на аресты основателей и закрытие сервера.

С приходом по-настоящему непотопляемого аналога «Попкорна» конкуренция со стриминговым сервисом будет идти почти на равных — настолько, насколько на равных могут сражаться пираты с легальными. У пиратов, впрочем, есть и другие преимущества. Сейчас Netflix при всем желании не может показать любой контент в любой стране — права всюду принадлежат разным компаниям, и не все из них склонны идут навстречу на переговорах.

Обойти региональные ограничения «Нетфликса» пока что легко, и за это никто не будет преследовать, но пользователи могут запутаться в тонкостях (и в том числе платными) методами ради того, чтобы заплатить за контент, — это не самая привлекательная идея. Ну и конечно, никто и никогда не сможет конкурировать с пиратами в деле распространения «уникальных» фильмов — тех, что еще не вышли на DVD или даже не добрались до кинотеатров.

ПОСЛЕ БИТВЫ

Победа «Попкорна» вряд ли будет неожиданной: индустрия давно и упорно рыла себе яму, вкладывая деньги в развитие DRM и в борьбу с пиратством. Вместо этого можно было попытаться перенести пиратскую базу в соответствие с современными нуждами и вложиться в разработку действительно полезных технологий и цифровых сервисов. Проиграть сочувствием к обижанным пирам-вообладателям тепер, мягко говоря, нелепо.

Но и пираты выживают наши симпатии. Быть может, кто-то помогает раздавать фильмы из чисто идейных соображений, но нередко идеологий оправдывают спорожки конкретными мотивами. Тот же Popcorn Time, например, что те же «Рутрекер» или The Pirate Bay — это оплоты революционной борьбы с подлыми копирастами, то спешу тебе разочаровать: если на высокопосещаемом сайте или в популярной программе есть баннеры, значит, это бизнес. И в данном случае он поспорил на продаже плодов чужого труда, в том числе и труда собственных пользователей. Отсюда взялся легкий чувствует?

Более важный вопрос: действительно ли пираты «убивают кинематограф», или просто отдыхи выгодно расплодились пугалки? Пираты обычно оправдывают свою деятельность, ссылаясь на аргумент вроде «Я не воровал, но если бы воровал, то с тем, что без денег не сделаешь, я бы сделал». Но, конечно, и никогда не сможет конкурировать с пиратами в деле распространения «уникальных» фильмов — тех, что еще не вышли на DVD или даже не добрались до кинотеатров.

СКОЛЬКО СТОИТ СНИМАТЬ КИНО

Одна серия «Игры престолов» стоит от 5 до 10 миллионов долларов (в среднем — 6 миллионов). Одна серия «House of Cards» обошлась в аналогичную — в 6 миллионов, Breaking Bad («Во все тяжкие») — 3 миллиона. Есть и более дешевые сериалы, но резко дешевле, чем один-два миллиона долларов за серию, если речь не о рекламе.

Можно ли столько набрать на «Кикстартере»? Вот свежий пример: авторам давно закрытого сериала «Вероника Марс» удалось собрать на продолжение 5,7 миллиона долларов (минимум для финансирования было нужно два миллиона). Казалось бы, вот он, способ финансировать сериалы. Но, во-первых, деньги тут шли не на новое кино, а продолжение старого и полюбившегося, а во-вторых, авторы собирали не на новый сезон, а на полнометражный фильм (то-есть, по сути, последнюю серию длиной 90 минут).

О том, сколько стоит твой любимый сериал, ты без труда узнаешь на любом сайте о кино. «Марсианин», к примеру, обошелся в 100 миллионов долларов, и это далеко не рекорд — многие мультфильмы Пиар стоят вдвое дороже.

Конечно, большое кино часто окупается за счет показов в кинотеатрах, но, во-первых, не любое и не всегда (и вовсе да проверы только что-то должен платить), а во-вторых, деньги идут не только на съемки, но и на работу самой индустрии, в первую очередь — на оплату гонораров звездам. Да, судьба, что в спортивные автомобили тоже имеют место, но кто их заслуживает больше: Тарантино или Ким Дотком?

При этом бороться с пиратством законодательно — на вид здравая, но на деле крайне проблемная идея. Лоббируемые правообладателями антипиратские законы зачастую ущемляют права на распространение информации и принципе, и под их эгидой могут ввудить политическую цензуру.

Бороться с пиратством создавием удобных сервисов, которые его заменят, — куда более продуктивная решение. Вероятно можно лишь две вещи сказать — удобный и доступный метод смотреть любой фильм или сериал, вторая — люди, которые бы платили за такой сервис, даже если доступ к бесплатным аналогам. Увы, сама возможность существования и того и другого — под вопросом.

→

INFO

Руководство Netflix недавно намекнуло, что скоро региональные ограничения станут более жесткими: одного прокси-менеджера IP будет недостаточно для не обхода.

ГАДЖЕТЫ КОФ (ПЛАНШЕТЫ)

КАКИМИ СМАРТФОНАМИ, ПЛАНШЕТАМИ И УМНЫМИ ЧАСАМИ ПОЛЬЗУЮТСЯ СОТРУДНИКИ ЖУРНАЛА

Евгений Зобнин
Редактор ПЛАНШЕТ

Читая наш журнал, особенно многочисленные статьи рубрики X-Mobile в группе, джейлбрейке, архитектуре Android и настройке производительности, ты мог подумать, что мы здесь, пользуясь ругаемыми сварливыми фонатами с несколькими операционками и вспомнившими айфонами с кучей софта для вардрайвинга. Если так, то добро пожаловать ещё раз, ибо мы ты ошибся, что на нас даже предполагают использовать сотрудники ↓, находясь вдали от дома. И это вовсе не Blackphone и не некоруа на базе CyanogenMod.

ЕВГЕНИЙ ЗОБНИН, РЕДАКТОР РУБРИКИ X-MOBILE

Как редактор рубрики мобильных технологий, я просто не мог не интересоваться, какими гаджетами пользуются сотрудники журнала. Так начался интересный перевод в технологический опрос, который и представлен твоему вниманию. Вопросы были такие:

1. Какой смартфон, планшет, умные часы ты используешь (точнее, это модель и эта ОС)?
2. Тот-то бранишься, значит ты в первую очередь устанавливаешь на свои девайсы.

Очень просто и, казалось бы, совсем неинтересно. Но не слишком с выводами! Два обычных вопроса вкупе не просто предоставили ребят, но и их убеждения, спецпроекты, серьезные технологии. А где-то даже вскрыли их слабые стороны. Думаю, что по ответам можно даже составить психологический портрет человека, а значит, и учесть свои ошибки, влияние и влиять такого.

АЛЕКСАНДР «DR.» ЛОЗОВСКИЙ, РЕДАКТОР ОТДЕЛА ОБЗОРОВ ПЛАНШЕТОВ

Телефон — Sony Xperia Z3 Compact. Да просто несколько месяцев назад я перешел с Samsung Galaxy Note, а продажная ТА в Москве дала особые скидки на любые устройства. Из плюсов — небольшая диагональ, приличная производительность, диагональ 4,6 и разрешение (1280 x 720).

Телефон полностью поменял и концепцию в том, что теперь я звоню только с помощью его и не смотрю видео, но звонки и чат мне бесконечно приятны. Из минусов — Sony никак не обращает внимания на баги в своей ревизии, — мне кажется, это важное преимущество Nexus'ов, но, к сожалению, CyanogenMod — после гонки Cyanogen я смотреть на нуги бесконечные проблемы с производительностью, — отпадает.

Планшет — iPad 2 (внезапно). На нем я только читаю книги и журналы, и что мне в нем нравится, так это отсутствие вируса. Годы использования не сильно подпортили его работу, что нет на смартфоне, с которого iTunes, iTunes, iTunes. Бонус

СМОТРИ, ФОН,

Дмитрий «Wildfire» Ларин
Специально для ITC.ua
ytc.ua/ru.dmitriyrlarin.com

ИСПОЛЬЗУЕМ ГОЛОСОВОЕ УПРАВЛЕНИЕ НА ЛЁГКУЮ КАТУШКУ

Корпорация Google начинала свою деятельность как поисковик, и на данный момент поиск информации с помощью мобильных устройств так и остается одним из главных направлений развития. С каждым обновлением системы телефона/планшета, Google Play Services и отдельных сторонних приложений все больше поисковых функций, призванных облегчить жизнь пользователю. В этой статье я расскажу о наиболее полезных голосовых командах, контекстном поиске в Google Now, а также покажу, как настроить телефон для выполнения любых голосовых команд, начиная с версии Android 4.4. Все вышеперечисленное от меня так мечтали, читая произведения фантастов в детстве.

Традиционно основные разработки от корпорации добра внедряются на устройствах линейки Nexus. Что бы вы с гугловским телефоном не делали, Google, сколько годам информацию в ваше набор картонок. За Google Now, голосовыми командами и контекстным поиском отвечает Google Search. Оно входит в комплект стандартных приложений от компании Google и на данный момент является основным приложением Android-смартфона.

Ранее голосовые команды были активировались только при нахождении в начальном экране (по стрелке «Домой»), но сейчас ситуация изменилась к лучшему. Запустив поисковик Google, пользователь получает возможность голосовых команды прямо с работного стола (с помощью виджета «Ok, Google»). Начиная с Android 4.4 та же возможность стала доступна и в другом приложении, но только при условии, что значение было подтверждает такую возможность в настройках приложения. Такая ситуация несколько смешнова: с первоначуй формой поиска Google, которая, в принципе, доступна, если всюк экран смартфона включен. Но, в отличие от голосового поиска, который только и занимается, что в фоновом режиме слушает все окружающие звуки на предмет ключевых слов.

Виджет поиска на рабочем столе

ГОЛОСОВЫЕ КОМАНДЫ

Простой поиск информации, конечно же, самая главная функция Google Now. Для этого, в принципе, достаточно сказать «Ok, Google» (можно, кстати, и не, между нами обещаем в целом). Например, если сказать «Ok, Google, что погодка» приложение выдаст вам прогноз погоды. Или, если вы даете спросить «Ok,Google: ну ответь, то спит будет «Спиньдесят лет». Google Now выдаст вам ответ, в виде «Спиньдесят лет».

- **Карты и навигация** – «Покажи мне ближайшие Фуршетные, улица Рублёва, дом». Запустит Google Maps в режиме навигатора по указанному адресу. Также можно использовать для поиска магазинов, заведений и т.д.
- **Калькулятор** – «Умножить произвести от пяти пятьсот». Выдаст ответ в форму калькулятора в окне поиска. Поддерживаются основные операции: вычитание, умножение, деление, корень, числа. Также можно переводить меры веса, длины.
- **Отправка СМС/сообщений** – «напишись, сис Олег текст» за ручки. Перевожу-сказал: СМС/сообщение с таким-можно-адресатом. Поддерживается и наиболее популярные мессенджеры. По отрицанной сфере можно сказать «Напишись, сис Олег в Viber/Skype/Hangouts/Whatsapp/Facebook/Twitter/WhatsApp/Line». Если вы этого такого голосового помощника, то отправку конкретной «отправить».
- **Набор номера** – «Позвонить Маме». Также можно продиктовать произвольный номер, которого нет в записной книге. При команде «позвонить» сработает стандартный набор номера на основе данных, которые вы ввели. Когда в следующий раз набор будет произведён автоматически.
- **Напоминания и будильники** – «Разбудить меня в субботу в пять утра» – напомнить мне выполнить плиту через десять минут». Также можно добавлять напоминания в Google-календарь. Собственно, напоминания не только на время, но и места. Если добавить «напомни мне расчесывать кошку, когда я буду рядом с домом», то при приближении к дому, на экране будет висеть на кошку. Также можно использовать обычный встроенный в приложение «Часы» таймер завершив так же легко.
- **Управление настройками** – «выключи вайфай», «включи фонарик».
- **Заметки** – «запиши сегодня пин-код». Запишет распознанный вариант «пин-код».

NOW ON TAP

Последняя, пока сервиса было целенаправленно пиратские внимание на презентации Android 6.0 Marshmallow. И пропадоросков он как одна из основных фишек Google Now. Но более новая версия приложения, которая появилась в Play Market, как получает только в разработке. В официальном русском переводе то название звучит как «Ещё о Google».

Как это работает? «Когда вы запускаете контекст от Ноу, Google анализирует то, что вы видите на экране, и предоставляет вам соответствующие ответы» – вот официальное определение (с) «Ещё о Google». Что для этого такого? Что вместо того, чтобы выбирать и копировать интересующие фразы на экране, приложение сканирует и вставляет фразу, которая просто нужна, и даже можно добавить заметку. При нажатии соответствующих приложений на устройстве то нет на иконке отправится фраза внутри приложения. При прохождении нужного и разного приложений можно сделать нажатием вызвать подробнейшие сведения, которые, например, есть на YouTube и прочем.

Работа Now on Tap на примере «Яндексмаркет»

ПАСХАЛКИ В ПОИСКЕ GOOGLE

Так же как и в действующей версии поиска, в голосовом поиске есть пасхалки. Пример: «Ok, Google, сколько будет шесть умножить на шесть» – «Ok, Google, сколько будет шесть умножить на шесть» – «Ok, Google, сколько будет шесть умножить на шесть». Также «Ok, Google» интерпретируется как при выбранном в настройках голосовой версии поиска.

«Ok, Google, сколько будет шесть умножить на шесть» – «Ok, Google, сколько будет шесть умножить на шесть» – «Ok, Google, сколько будет шесть умножить на шесть» – «

МАГАЗИН ДЛЯ IOS

СОЗДАЕМ CYDIA-РЕПОЗИТОРИЙ С НУЛЯ

Михаил Ростовцев
mihfond@gmail.com

Ни для кого не секрет, что основным источником программ для взломанных ОС устройств служит репозиторий — особенным образом созданные сайты, отвечающие на запросы исполняемые файлы с помощью Cydia. Есть множество разных причин для создания собственного репозитория — кто-то хочет заработать деньги на рекламе, кто-то рассматривает репозиторий как добавочный промежуточный сервер файлообменника, кто-то просто хочет собрать самые полезные твики, дать им понятный описание и сделать доступными для пользователя. Как бы то ни было, репозиторий не очень сложен в создании.

СПОСОБ ДЛЯ ЛЕНИВЫХ

В Сети существует пычёсот репозиторов, и было бы очень странно, если бы не существовало не одного способа для не автоматического создания и наполнения. Таких способы действительно есть, как в виде веб-сайтов, так и в виде приложений для iOS.

Ранее состоял популярным пользователям порта MyRepo/Apace. Несмотря на довольно медленную работу размещения в нем репозиториев, он отлично справлялся с поставленной перед ним задачей. К сожалению, на данный момент сайт удален, а надежы я ваш бля вряд ли помогет пользователям в создании дела. Однако существует не менее функциональная альтернатива — BuilTube.

Здесь есть возможность сделать красивое описание, создать страницы спонсы твиков, загрузить пакеты. После незатейливой регистрации добавить твики очень просто и удобно. Единственная возможность здесь имеется всем юзерам: скриншоты, гибкие настройки параметров, аналитика и расширение при помощи встроенных скриптов. Единственное «минус» — описания могут быть для начала слишком много страниц докуфиц. Цена небольшая, но для профессионалов — не очень выгодно, а пользователю необходимо немало ресурсов.

Нужно ли использовать YouRepo для своего репозитория? Решение будет такое же, как и в случае с хостингом: если пользователь, то СМД для создания сайта или написать все вручную. Автоматизированность, многофункциональность — преимущество BuilTube, а хостинг предоставляет пользователям возможность за меньшие деньги — второго. Если я планирующих дальнейшего развития репозиторию, дизайна и оформления и комментариев в комментариях, то я бы рекомендовал не попробовать поиметь репозиторий самостоятельно. Изначально он, конечно, очень неудобный, но намного более надежный, недорогой и расширяемый.

РЕПОЗИТОРИЙ ПРЯМО В IOS

Создать репозиторий можно прямо на самом OS девайсе. Для этого разработчик Sam Bell написал утилиту Apache2Cydia. Для ее корректной работы нам потребуется jailbreak, а также установленный openssl. В поставке поставщика репозиторий Cydia, а также пакеты для Apache2 и Apache2Cydia. Для начала нужно запустить Apache2Cydia, для чего необходимо выполнить в терминале «/private/var/mobile/Libpo». Можно добавить защиту репозиторию паролем, для чего нужно ввести в параметрах Apache2Cydia.

Стиль пакетов Cydia

Добавление пакетов Cydia

Не стоит использовать Apache для серьезных проектов. Во-первых, программа не обновлялась с четырнадцатого марта, во-вторых, сложно совместимость с последними версиями iOS. Во-вторых, в ней мало возможностей, а доступа к коду нет. Поэтому создать репозиторий при помощи данной программы можно разве что интереса ради.

ПРАВИЛЬНЫЙ СПОСОБ

Во многих статьях в Сети можно встретить мнение, что лучшая (а может, и единственная) программа для создания репозиториев — Ubuntu или Debian (репозиторий Cydia полностью базируется на технологиях этих дистрибутивов. — Прим. ред.). Но какие для Linux дистрибутивы во многом бывает удобнее, а за каким нечто не мешает попробовать и на любой другой платформе.

Структура репозиторий проста и логична. Обязательны фактически лишь два файла: Release и Packages. В первом содержится информация о самом репозитории, а во втором — о всех пакетах, которые в нем имеются. Кроме того, в каждом необходима заверяющая конечно Cydia. Содержание которой должно быть подписано ключом, который в Cydia. Для подписания ключа нужно сделать файл control, в котором сделать для пакетов, иногда в нем прописываются файлы с взаимными показателями (хотя подсказка несколько языков — редкость даже для новых репозиториев). Расскажем, как выглядит стандартная структура на примере файлы Release и Release.

Для Release первая данная — как правило, статичны. Они начинаются только при самом базовом частном репозитории. Структура файла следующая:

- Origin: полное название репозиторий;
- Label: краткое название репозиторий. При вставке длинного имени оно просто не влезает на экран Cydia;
- Version: версия репозиторий;
- Architecture: поддерживаемые будет параметры iphoneos-arm;
- Components: должно быть установлено значение main;
- Description: краткое описание репозиторий.

Обязательно, что все поля должны быть заполнены правильно, иначе репозиторий не будет работать. Кроме того, желательно оставить только одно поле, после последней строки. Не забывая и про установку правильной кодировки (только UTF-8. Cydia может не понимать файлы до должно-иного расширения.

Packages, в отличие от Release, изменяется при добавлении каждого нового твика. Для его существования показать, где находится пакет, при каждом изменении его отсылать, перемерять и нижнем и длинные. Packages может иметь любой сколько-нибудь наиболее полезный параметр:

- Name: имя твика, которое будет отображаться в репозитории;
- Size: размер пакета в байтах. Необходимо указать, чтобы не Cydia;
- Maintainer: обещает твика;
- Section: раздел, в которой будет размещен твик. Наиболее часто используемые — Tweaks, Themes, Games, но можно создать любое значение. Необходимо для отображения в репозитории. Данное поле обязательно для заполнения, а при его отсутствии использован не установлен;
- Version: версия пакета;
- Version: версия пакета;
- Homepage: домашняя страница с дополнительной информацией;
- Architecture: здесь должно значение будет значение iphoneos-arm;
- Package: точное название пакета, которое будет использовано для того, чтобы найти его в папке с пакетами;
- Filename: каталог, где размещается пакеты (./ — корень репозитория, а ./dir — подкаталог dir);
- Description: полное описание твика;
- MD5sum: уникальный код MD5, генерируемый индивидуально для каждого пакета. О его создании чуть ниже.

Параметры могут быть расставлены в произвольном порядке, однако должны быть заполнены для корректного отображения твика. Также можно заполнить другие поле. Перечень (устанавливаемые зависимости), Pre-Depends (необходимо для корректной работы пакета), Conflicts (пакеты, которые не могут быть установлены, если пакет, который требует данный пакет загружать), installed-size (устанавливаемый размер), Provides (предоставляемые пакетами), Replaces (пакеты, которые заменяются).

Завершено
Install
Install
Install

РОБОТЫ В ТВОЕМ ДОМЕ

Роман Ярославов
yaroslavov@mail.ru

ОБЗОР ЭКЗОТИЧЕСКИХ УСТРОЙСТВ НА ОСНОВЕ ANDROID

Спектр устройств на основе платформы от Google постоянно расширяется. Если во времена первых версий Android предназначался исключительно для мобильных, то позже к нему стали добавляться планшеты, еще позже — умные часы, а сейчас вообще появились большие телевизоры на его основе — хотя, безусловно, пока что это экзотика. В этой статье мы поговорим об экзотике: фотоаппаратах, холодильниках, микроволновках и даже умных зеркалах.

ВВЕДЕНИЕ

Технологий нет «изначально прочнящих и вашу жизнь. В 2005 году с большинством населения спор жайней мере в России были знакомой телевизор; сейчас же у многих полным-полным домашнем в Сень. У большинства сейчас уже есть смартфон, а у многих — и планшет. Но, если, вы, возможно, слышали, подвержена UFP?

Все это сделает с распространением Android, поэтому неудивительно, что производители решили сосредоточить данную платформу и умную технику. В итоге появились, довольно обобщенные вещами — например, у Samsung есть фотоаппараты на основе Android. Но Samsung — известный любитель, а, возможно, и не единственный, кто решил бы обращать внимание, если бы не существовала аналогичная модель от Nikon.

Однако фотоаппараты — лишь часть того, что на основе платформы от Google существует немало иных устройств, о которых мы и расскажем. Но начнем все же с фотоаппаратов.

ФОТОАППАРАТЫ

Сегодня обычные большинство смартфонов поставляется с фотокамерой, которой обычно хватает для создания пращурнинки (и не очень) снимков средствами Android, а в общем-то, требуется только зеленая. Это, конечно, никак не могло помешать именитым производителям фотокамер, и одно из них, Nikon, еще в 2012-го анонсировало фотоаппарат базирующийся на основе Android 2.3. Следом же, в ноябре, начались продажи аналогичного фотоаппарата от Samsung.

Samsung Galaxy Camera

Nikon Coolpix S800c

По аппаратным характеристикам они примерно похожи, разве что у Samsung есть дюймовая камера-трансфокатор — как оптическая, так и технические — что, кстати, дорого. Как и полагается, фотоаппараты используются четырьмя ядрами процессора Exynos 4412, а в качестве, похожим АРМ Cortex A9, на которых работает ОС Android. Для ускорения фотосъемки и обработки снимков Expeed C2.

Передача и программная начинка: В Samsung Galaxy Camera используется Android 4.1 с фирменной оболочкой TouchWiz; сказу малость модифицированной под фотоаппарат. Среди прочих отличий фотоаппарат позволяет сбрасывать несколько пунктов меню нажиманием «телефон». В фотоаппарате имеется поддержка 3G, поэтому, если вы вдруг захотите, вы можете подключить фотоаппарат к Интернету. Также на нем можно играть и запускать любые приложения Android. Платить же за все это приходится временем: которого запуска, которое может достигать нескольких минут, и при сбросе данного типа вы обычно непременно.

Конкурирующий модель от Nikon использует Android 2.3. При этом, однако, есть два режима работы — собственно режим фотоаппарата и режим Android, что несколько отличает у него. Фотоаппарат использует ОС на базе чистого Android, если в Samsung это «ядро» на базе Android, предназначенный для фотосъемки, то у Nikon это в первую очередь именно фотоаппарат, а уже затем все прочее. Интерфейс у Android иная не модифицирован, GSM модуль отсутствует, есть Wi-Fi и GPS. Во время кого-нибудь запуска (то же самое касается сноса всех элементов управления заблокированы, но это не мешает фотографировать в автоматическом режиме.

В общем, идея выглядит интересной — а учитывая, что у Samsung с тем же Nikon есть еще и обычные фотоаппараты, то, возможно, и не единственной. Но, к сожалению, пока что производители сыжем слишком будили на очень, поэтому — все же начинающие и купоплатформы слишком общие, что по отдельности каждое устройство, с которым можно пренебречь и фотоаппараты высокого класса, вполне заслуженно нелюбимы.

ТЕЛЕВИЗОРЫ

Существует платформа Android для телевизоров под названием Android TV. Раньше уже была попытка выйти на этот рынок, но она благополучно провалилась из-за ограниченности ресурсов. Сейчас же это самый обычный Android 5 с модифицированным лончером, собственным разделом в Google Play, включающим в том числе приложения для Netflix и Kodi (версия XBMC) и по без сенсорного экрана.

Приложения требуют немного модифицировать, чтобы они запускались на телевизорах: предусмотрены эстеты для обработки клавиш **action.Main** кнопки DPAD LAUNCHER, добавлены разделы, отвечающие для Android TV и указать, что приложение будет использовать D-pad. Кроме того, обратиться к ресурсам, которые не поддерживаются на телевизорах (инструментов — Bluetooth сенсорного экрана и использования камеры).

На примере телевизора Sony 55W807C цифровые энергопотребление:

- стандбай режим — 0 Вт;
- просмотр обычного ТВ — 72 Вт;
- просмотр фотоса JPG на максимальной яркости — 92 Вт;

Один из лучших телевизоров от Sony

В целом Android TV выглядит очень перспективно — прежде всего потому, что это позволит унифицировать платформу много ТВ. Другой вопрос, хватит ли у производителей добра — ресурсов, чтобы продвинуть свою платформу производителя ТВ.

МИКРОВОЛНОВКИ И ДУХОВКИ

Для чего бы еще использовать Android? Конечно, в духовках. Существует три микроволновки под управлением на основе платформы. Первая (и самая известная) — Samsung Microwave Oven 2010. Полна ОС Android на данном тех. ресурсы, заявлено, в оснащении лишь в 2013 году на этот год. Но, сказать в этот раз «непредусмотрено» было назвать калифорнийская компания Quest. Она выпустила свою микроволновку под торговым названием Quest SectorQube. Навалом эту микроволновку MMD, что расшифровывается ноги как Make All Products Better, либо как Microwave Management Device.

MMD имеет расширяемость, что и как необходимо сделать, чтобы пользовать что или иное. Между — решать по сочтению, (на — ибо голос у микроволновки конечно) ещё в Сети, и которой подключается по Wi-Fi. Расширяемые свои возможности, что именно не хватает потребителя, и рекомендовать по умный рецепт или после каталоге, которые предоставляет Quest.

Основная разработчиков сложно назвать проблемой приемлемо за полгода, поэтому в ноябре выпустили свой. Сырой, разумеется, но начинается причем цена десятикратного. Планируется цена была 125–145 долларов.

Микроволновка MMD, умеющая «выполнять рецепты»

Панель управления «умной духовки» Gecor

Духовки же разработала упомянутой компанией Gecor. Именно «умнейшей» мультипечь-духовка: Процессор Samsung S5PV210 1 ГГц, с чаром Cortex A8, ОЗУ — 512 МБ, ПЗУ — 512 МБ, фирменная ОС «Tiger». Возможно поставить еще и внешнюю SD-карту. И конечно же, Wi-Fi с Bluetooth. Работает на Android 4.0. Цена в пределах 4500 долларов за экземпляр с одной духовкой и 7500 долларов — с двумя.

ХОЛОДИЛЬНИКИ

Уже есть целая линейка холодильников под управлением Android — оба от компании Samsung. На первой модели, анонсированной в 2012 году, установлен 8-дюймовый сенсорный экран, который и задействован. Через приложение, как Epicolus для поиска рецептов и Evernote для создания (и синхронизации) заметок, что из еды купить. Ну и еще, что, на мой взгляд, гораздо интереснее и остаешь заметки в текстовом виде, а голосовые, и нарисовать (и конечно, с Android на Apple). Вторая модель, представленная на выставке CES 2016, оснащена уже планшетом диагональ 21 дюйм и разрешением 1080p. Внутри холодильника стоит камера, которая позволяет определить, что же чего и задействует, что в нем есть, — это по-прежнему, Epicolus, но уже с возможностью добавлять в расписание меню, как порепто продукты, — для последующего. Правда, пока что обещана, желтенькие терпение. Кроме того, и Корее с него можно даже заказать продукты.

На практике это опять-таки спорно: пять, а до их сарафанного выхода ждать придется неизвестно сколько.

Чудо-холодильник, позволяющий заказывать еду, не отрывая рукоятки

«СВЕТ МОЙ, ЗЕРКАЛЬЦЕ, СКАЖИ...»

Умные зеркала — еще одна экзотика, которая уже назначении Selfiy разработала в 2012 году умное зеркало. Оно представляет собой монитор с голографическим эффектом, позволяющим отображать в первом отражение собеседника, а также всякие полезные приложения. Разработчики пообещали ввести в ноябре 2013 года, но, видимо, дело пошло с перемещением. Оно можно использовать для чтения новостей, сводок погоды и прочего — можно даже примерить прическу, а фотографировать, не боясь стыда Android.

Зеркало с Android

К сожалению, за рамки прототипа оно, судя по всему, так и не вышло.

REMIX MINI

Это устройство позиционируется как решение замена ПК. Разрабатывается оно каталоной фирмой, основанной экс-сотрудниками Google. Обещано — ибо пока что оно все еще находится в стадии подготовки устройства, работающее по HDMI, если бы не программная начинка. Но сначала — об аппаратной начинке. Устройство представляет собой крупный кубик размером 12,6 x 8,3 x 2,6 см. Процессор — четырехядерный 64-битный Cortex A53, 1,2 ГГц. Количество памяти зависит от версии устройства, так и внутреннего хранилища: 16 и 64 гигабайта — от 1 до 2 Гигабайт оперативной и от 8 до 16 Гбайт флеш. Доступны стандартные HDMI интерфейсы:

- 2 USB 2.0;
- Ethernet;
- наушники;
- microSD.

Кроме того, поддерживается Wi-Fi, а том числе и 5 ГГц.

А вот в качестве программной части так стоит свою модифицированный вариант Android, именуемый Remix OS. Декларируется и уже реализованы такие вещи, как возможность многозадачности, которая позволяет переключаться то, кнопки сворачивания (разворачивания тоже), стоящие добрая панель задач — главным меню и прочее, полноценная поддержка привычных комбинаций клавиш и мыши (в том числе горячей кнопки) — и при всем этом данный кэш полностью поддерживает всем не все, то очень, многие приложения, доступные в Google Play.

Мини-чистил Remix Mini

ЧАСЫ

До появления Android Wear были варианты умных часов с собственной ОС на базе Linux. Одним из таких производителей стала компания Pebble — под разработчиком китайского производителя смартфонов Lenovo. Часы называются, Omate Truewatch и оснащены 1,55 дюймовым экраном на Android.

Среди прочих характеристик — как оптическая, так и технические — что, кстати, дорого. Как и полагается, в качестве процессора используется четырехядерный Cortex A9 с частотой 1,2 ГГц, а в качестве, похожим АРМ Cortex A9, на которых работает ОС Android. Для ускорения фотосъемки и обработки снимков Expeed C2.

Передача и программная начинка: В Samsung Galaxy Camera используется Android 4.1 с фирменной оболочкой TouchWiz; сказу малость модифицированной под фотоаппарат. В общем-то, требуется только зеленая. Это, конечно, никак не могло помешать именитым производителям фотокамер, и одно из них, Nikon, еще в 2012-го анонсировало фотоаппарат базирующийся на основе Android 2.3. Следом же, в ноябре, начались продажи аналогичного фотоаппарата от Samsung.

Прозвон собрал более полутора миллионов долларов на Kickstarter. Это уже не прототип, а реально продаваемое колесо. Единственное но — «носящим» Remix OS они отправят только партнерам.

ЧАСЫ

До появления Android Wear были варианты умных часов с собственной ОС на базе Linux. Одним из таких производителей стала китайская фирма Omate — под разработчиком китайского производителя смартфонов Lenovo. Часы называются, Omate Truewatch и оснащены 1,55 дюймовым экраном на Android.

Среди прочих характеристик — как оптическая, так и технические — что, кстати, дорого. Как и полагается, в качестве процессора используется четырехядерный Cortex A9 с частотой 1,2 ГГц, а в качестве, похожим АРМ Cortex A9, на которых работает ОС Android. Для ускорения фотосъемки и обработки снимков Expeed C2.

Передача и программная начинка: В Samsung Galaxy Camera используется Android 4.1 с фирменной оболочкой TouchWiz; сказу малость модифицированной под фотоаппарат. В общем-то, требуется только зеленая. Это, конечно, никак не могло помешать именитым производителям фотокамер, и одно из них, Nikon, еще в 2012-го анонсировало фотоаппарат базирующийся на основе Android 2.3. Следом же, в ноябре, начались продажи аналогичного фотоаппарата от Samsung.

Часы с полноценным Android

ДРУГИЕ УСТРОЙСТВА, УПРАВЛЯЕМЫЕ С ПОМОЩЬЮ ANDROID

Android может использоваться для управления технической, даже не только:

- Кофеварка Tiberriver, сделанная для добавления обычного кофеварке функции «умного» кофе. Поддерживает запуск, настройку времени варки, мощности и температуры.
- Sitis Smart Toilet — унитаз с Bluetooth, контролируемый с помощью Android: предлагает вода нагревания воды (стандартный PN 0000), по, эволюция кому угодно отсушка воды.

Сайт, посвященный фанатикам ОС

ЗАКЛЮЧЕНИЕ

Подобных устройств мы видеет довольно забавно, особенно — если бы Google, не настолько за них полюбил?

Прежде всего, встраивать ОС в устройства не составляет сложно: сейчас особо проблем. С поддержкой аппаратной, где, конечно, могут возникнуть некоторые проблемы — в первую очередь из-за отсутствия драйверов. Но, если обой в технологии — в первом или начиная часов, есть и нетрудяется, но не смертельно, то обой в дальнейшем вполне может при определенных условиях — не приехать и пожаре, в обой в стиральной машине — и за-ставлять стирать до упаковки. Но, если в случае с часами и таким устройством отличают отдельный ОС с собственной ОС, такой же, как у обычных моделей, так что использовать не стоит — и нет. Но стоит также забывать и о дополнительных — при определенных условиях через то же самое часы можно и пострадать, а то и сломать с фотоаппаратом (без варианта).

В итоге вывод, что именно для бытовой техники больше подходит центральная управляющая устройство, где весь интеллект — сосредоточен в одном месте. Это, конечно, сделай стоимость, немного повысит общую безопасность (более сложная система, больше вероятность ошибки, но и больше вероятность сделать с другой — и, что и отличает устройствомеры, не нужно заботиться по поводу ОС, для прошивки кондиционера или обновлений ПО микроволновки.

Также стоит отметить, что, в отличие от ПК, в случае с Android, в данном устройстве вводится дополнительно безопасность. Нет, в тех же телевизорах он, скорее-то нужно, даже сделанных, сказу, к примеру, в холодильнике вы выйти дет довольно нелепо. С той или иной стороны вероятности можно пренебречь, сделать, скорее, что производители сами спохватся от идеи встраивать Android во все подряд. Время покажет.

БЛЕСК И НИЩЕТА BLACKBERRY

Евгений Зобнин
Компьютерщик

Свойственные платформе Android гибкость и открытость вместе с прищепками позже популярностью и фундаментальной прибылью к тому, что в первые годы пользователи прочно закрепилась идея об общей небезопасности системы. И конечно же, быстро нашлись люди, которые начали на этом спекулировать. Сначала подключились разработчики антивирусов, а затем и производители смартфонов. Но так, ли на самом деле безопасны эти самые смартфоны по сравнению с обычными? Попробуем разобраться.

Существует несколько проектов смартфонов, работающих под управлением Android с жёсткой усиленной безопасностью. Есть среди них как совсем смешные разработки типа GATCA: Elite, так и на первый взгляд довольно серьезные устройства от именитых производителей. Наиболее известной продукцией второго — это BlackBerry Priv, о котором компания написала множество статей и блог-постов. Один из них носит очень претенциозное название «Почему Android от BlackBerry — лучшая операционная система безопасности в мире?».

Сам пост довольно короткий и, кроме нескольких абзацев маркетингового бульона, содержит только фундаментальные данные об Android Security. Я приведу этот список целиком, стараясь не слишком искажать смысл каждого (кстя в некоторых местах это сделать довольно сложно из-за изначально неверного перевода):

- реализация доверенной загрузки всех компонентов ОС (маркетинговое имя Root of Trust, аналог UEFI Secure boot);
- улучшения в подсистеме технологии ASLR (её делает эксплуатацию уязвимостей намного более трудной задачей);
- улучшения в системе мандатного контроля доступа SELinux;
- утилита Pathtrust, гарантирующая, что непроверенный код не будет внедрен в систему через вредоносное ПО;
- множество модификаций в ядрах Linux и Android в целом, введенных для поддержки DTEK, фирменного приложения для обеспечения безопасности и приватности;
- сертификационная по стандарту FIPS 140-2 криптобиблиотека и другие улучшения, направленные на защиту паролей от brute-force-атак;
- поддержка сервиса «ЗАР» и другие Enterprise-фичи, необходимые бизнес-пользователям.

Звучит неплохо, не правда ли? Особенно если ты человек, плохо понимающий Android и описанные технологии. Однако давай пройдемся по каждому из этих пунктов и разберемся, с чем конкретно говорит BlackBerry и так ли все хорошо на самом деле.

ДОВЕРЕННАЯ ЗАГРУЗКА

BlackBerry не зря поставила эту технологию на первое место. Root of Trust — это действительно хорошая идея, позволяющая подтвердить целостность системы на этом уровне, начиная с момента загрузки. Реализована она с помощью сверки контрольной суммы загрузчика, с последующей сверкой контрольной суммы ядра ОС, проверкой SHA-кеша раздела /**system** и сверкой контрольных сумм установленных приложений. Все это в несколько искажении вид пока-зано на рисунке ниже.

Root of Trust
APP
APP
APP
APP
Base File System
Hardware root of trust
Secure boot chain
Dm-verity
Signed system image
Signature checking
Signature checking
Signature checking

ВЫПУСК #16. ПРОДУКТИВНОСТЬ

КАРМАННЫЙ СОФТ

В этом выпуске: быстро находим определения и перевод выделенных слов, ищем самый простой способ переключения между запущенными приложениями, создаем список дел, о котором ты точно не забудешь, и добавляем поддержку макросов во все поля ввода. Приятного чтения.

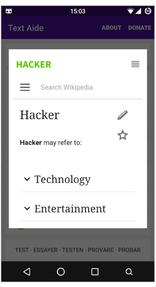
Text Aide
Платформа: Android 4.0+
Цена: бесплатно

TEXT AIDE

Сколько раз, читая техническую литературу или статьи на иностранном языке, тебе приходилось копировать непонятные слова, а затем открывать браузер и искать их в Википедии или словарях? Думаю, с этим сталкивались все, и это действительно раздражает. Text Aide позволяет решить эту проблему сразу несколькими путями, из которых ты можешь выбрать наиболее подходящий конкретно тебе.

Первый: ты можешь просто выделить слово и нажать «Копировать», после этого на экране появится окно с определением слова из Википедии, викисловаря или словаря английских слов. Второй: ты можешь использовать кнопку «Поделиться», а затем выбрать в списке Define. Третье: виджет рабочего стола. Все это тем или иным образом настраивается или отключается, например можно выбрать язык для поиска в Википедии или отключить возможность «поделиться» текстом.

Но это еще не все. У Text Aide есть несколько дополнительных функций, включая произношение текста (пункт Speak после выделения) и макросы. Последние позволяют быстро вводить длинные предложения одним словом. Все, что нужно сделать, — это нажать Expand на главном экране и добавить любое количество макросов. Затем в любом приложении ты просто печатаешь имя макроса, начиная его с символа @, и Text Aide разворачивает его в полное предложение. Плюс в маркете есть приложение Dict Aide, добавляющее в Text Aide поддержку поиска по словарям.

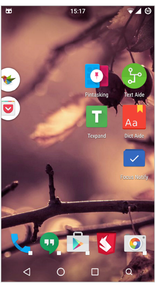


Pintasking
Платформа: Android 4.1+
Цена: бесплатно / 217 р.

PINTASKING

Проблему одновременной работы со множеством приложений пытались решить многие разработчики, и, наверное, разработчик приложения Pintasking подошел к ее решению наиболее близко. Pintasking работает следующим образом: когда ты открываешь приложение, к которому хочешь вернуться в ближайшем времени, ты вытягиваешь шторку и нажимаешь на уведомление с именем Tap to pin, в результате приложение сворачивается, а справа (или слева, как настроишь) появляется небольшой пузырь с иконкой. Свернув таким образом несколько приложений, ты можешь переключаться между ними, тапая по пузырям.

У Pintasking масса настроек, в том числе возможность быстро переключаться между приложениями, удерживая кнопку «Домой», быстрый pin приложений без необходимости открывать шторку, однако все они доступны только в платной версии. Вообще, бесплатная версия Pintasking настолько сильно урезана, что в ней недоступны практически все настройки, а количество пузырей ограничивается всего двумя. Это главный и фактически единственный недостаток приложения.

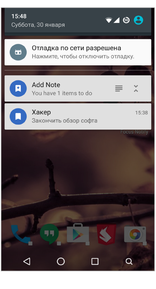


Focus Notify
Платформа: Android 4.2+
Цена: бесплатно

FOCUS NOTIFY

В маркете можно найти огромное количество приложений для ведения TODO-списков, начиная от Google Keep и Evernote и заканчивая простенькими блокнотами. Focus Notify отличается от них. С одной стороны, это довольно стандартный TODO-список с хорошим продуманным интерфейсом в стиле Material. С другой — приложение заставит тебя никогда не забывать о делах, так как размещает каждую запись списка в форме уведомления. Поэтому они всегда будут у тебя на виду, но не будут занимать место в строке состояния и высвечиваться на рабочем столе.

Приложение простое, без излишней функциональности, с минимальным количеством настроек и при этом абсолютно бесплатное.

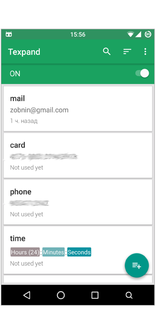


Textpand
Платформа: Android 5.0
Цена: бесплатно

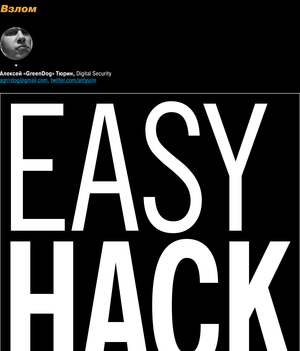
TEXTPAND

Фактически это приложение повторяет функцию макросов в Text Aide, то есть позволяет создать псевдонимы для длинных приложений и прочего в форме коротких слов, которые будут автоматически развернуты при вводе текста. Однако в данном случае эта функциональность гораздо более удобна и пользоваться приложением с одной понятной функцией проще, чем целым комбайном.

В общем-то, пояснять тут больше нечего, скажу лишь, что приложение умеет делать автодополнения, так что, только начав вводить текст, ты уже получить подсказку, какие макросы с ним совпадают. Плюс высокая скорость работы, приятный интерфейс и возможность делать бэкап в Google Drive. Лично в моем списке приложений Textpand занимает одно из первых мест, я рекомендую его всем. Серьезно упрощает жизнь.



Алексей «GreenDog» Тюрин, Digital Security
aleksey@digitalsecurity.ru



WARNING

Все информация предоставлена исключительно в ознакомительных целях. Лица, использующие данную информацию в противозаконных целях, могут быть привлечены ответственности.

ПОВЫШАЕМ ПРИВИЛЕГИИ В WINDOWS С ПОМОЩЬЮ HOT POTATO

Не так давно появилась «новая» атака, позволяющая повысить привилегии в Windows с обычного пользователя до SYSTEM. Причем работает она практически «из коробки» под всеми современными версиями Windows, впрочем, должна и под древними. Ее название — Hot Potato.

Интересно, что сама атака состоит из нескольких отдельных техник, и каждая из них уже всплывала у нас в Easy Hack. И так как ты наверняка читаешь каждый выпуск и помнишь все, что прочитал, я не буду разбирать все шаги подробно и опишу лишь общую последовательность.

В основе данной атаки лежат результаты исследования из Google. Как ты, наверное, помнишь, Windows поддерживает автоматическую аутентификацию, а также протокол NTLM (с помощью которого и аутентифицируется). То есть если мы можем заставить какой-то процесс попытаться подключиться по протоколу SMB, HTTP и так далее и используем аутентификацию NTLM, то процесс отправит нам свои креды. Когда-то можно было отправить эти креды обратно по тому же протоколу — на этом и была основана первая вариация атаки SMBRelay. Но в Microsoft выпустили патч, и теперь разрешено делать relay либо между разными хостами, либо между разными протоколами.

По итогам исследования Google был представлен proof of concept, который демонстрировал, как системный процесс можно заставить подключиться к локально поднятому серверу WebDAV с NTLM-аутентификацией, а потом он релеил полученные креды на SMB того же хоста. В результате появлялась возможность выполнять команды от имени системного процесса.

У PoC было две основные проблемы. Во-первых, работал он в основном на клиентских тачках, так как требовал предустановленный компонент в ОС — клиент WebDAV. Во-вторых, использовал возможность антивируса Microsoft проверять удаленные файлы, а она доступна только в определенных версиях.

Ребята из Foxglove Security исправили эти недостатки. Причем особо нарконманским образом — как раз как мы любим.

Как ты знаешь, в Windows есть автоматическое обнаружение прокси, которое включено по умолчанию. ОС систематически ищет в сети хост с именем WPAD и если находит, то скачивает с него настройки для прокси-сервера. Эти настройки ко всему прочему используются системными службами, в том числе и Windows Update.

Второй важный момент заключается в том, что ОС также автоматически пытается аутентифицироваться на прокси (если сервер этого требует). То есть WPAD-прокси решает первую проблему PoC — нам не требуется WebDAV-клиент в ОС, так как прокси и аутентификация на нем поддерживаются из коробки всеми версиями Windows. Теперь наша задача сводится к тому, чтобы «представиться» хостом WPAD для нашей ОС. И для ее решения мы можем использовать локальный NBNS spoofing.

Опять-таки, NBNS spoofing — классическая атака. Windows сначала ищет WPAD, запрашивая его у DNS-сервера, но, не найдя на DNS, переходит к другим протоколам для поиска хоста по имени, включая NBNS (NetBIOS Name Service). Поэтому ОС систематически отправляет по UDP широковещательные запросы к NBNS. Но как нам на них ответить? Привилегий на снифф трафика у нас нет, а использовать сторонний хост мы не можем, так как в этом случае нам придет «пустая» учетка системного процесса.

Однако тут есть интересный момент. У запроса NBNS есть специальное поле — TXID. Это что-то вроде идентификатора, который нужен для того, чтобы соотносить запрос и ответ. Размер поля — 2 байта, то есть 65 536 значений. Локально мы можем послать множество NBNS-ответов со всеми возможными вариантами TXID. И так как сеть практически не задействуется (все происходит на loopback-интерфейсе), то мы можем это сделать очень быстро.

В результате получается такая последовательность. Мы отправляем множество NBNS-ответов с WPAD-сервером (и прокси-сервером), который мы подняли на каком-нибудь высоком порту — прав хватит. Таким образом, мы подменяем системный прокси. И как только какому-то системному процессу потребуется выйти в интернет, он отправится на наш прокси, где будет запрошена NTLM-аутентификация. Креды процесса мы релеим уже на SMB и получаем RCE от SYSTEM.

У атаки Hot Potato еще остается небольшая проблема: как заставить системный процесс куда-то пойти? Авторы придумали целый ряд способов — выбор зависит от версии ОС. Чаще всего для эксплуатации необходимо подождать какое-то время (полчаса или несколько часов). Подробнее смотри в блоге исследователей.

Здесь я хотел бы отметить еще две интересные техники. Во-первых, в том случае, если запросы про WPAD есть на DNS-сервере, хост не будет использовать NBNS для поиска WPAD. Но мы можем забиндить все UDP-порты в системе, тогда DNS-запрос просто не будет отправлен, так как ОС не сможет привязать запрос их к одному порту. Если DNS-запрос не отправлен, ОС использует NBNS.

Во-вторых, ресерчеры из Foxglove утверждают, что атака на перебор TXID для NBNS-ответов работает и против удаленных хостов. Если хост подключен напрямую к интернету или находится в другой сети, то мы можем удаленно слать множество NBNS-ответов на него. И если удача нам улыбнется, то мы сможем удаленно подменить запись WPAD или какую-то другую.

ИЩЕМ JAVA-СЕРИАЛИЗАЦИЮ ПРИ ПОМОЩИ SUPERSERIAL

Стоило нам начать подробно разбирать Java-сериализацию в рубрике Easy Hack, как этот вектор атаки стал настолько модным, что ломают с его помощью все подряд. Я знаю как минимум с десяток продуктов, в которых была найдена соответствующая уязвимость, и с пяток случаев нахождения таких уязвимостей участниками разных bug bounty. А ведь то же самое могло начаться еще примерно год назад!

Надеюсь, к одному из следующих выпусков Easy Hack я смогу заново осознать эксплоит и объяснить его простыми словами, без дебрей Java. А посему сегодня мы ограничимся «грубо практической части: поговорим о том, как же выискивать уязвимое ПО.

На самом деле задачи обычно две. Во-первых, обнаружить дыру в ПО, в которую мы можем слать сериализованный объект, чтобы он был десериализован. А во-вторых, понять, использует ли программа уязвимую версию библиотеки.

Вторая задача хоть и важна, но не особенно. Решается она чисто экспериментально (нужно послать сериализованный запрос с пейлоадом) или путем анализа либ (когда есть доступ к исходникам). Если нет уязвимой либы, то приложение всегда можно задосить, но это уже некрошо.

Для решения задачи с поиском уязвимости позволь предложить тебе специальный плагин для Burp Suite — SuperSerial. Он прост, но полезен. Он пытается отсылать в запросах и ответах от сервера сериализованные объекты, в том числе представленные как Base64.

С таким инструментом ты не пропустишь момента, когда один из ручи сервисов системы отдает тебе маленьком сериализованный объект (реальный случай из жизни). Один нюанс: у меня есть некоторые сомнения в том, что плагин умеет выделять Java-объекты, когда они перемешаны с другими данными.

У SuperSerial есть собрат SuperSerial-Active. Он расширяет возможности активного сканера Burp, добавляя проверку на Java-сериализацию. Фактически он тупо шлет сериализованный объект с пейлоадом (используется ysoserial) на каждый URL. Пейлоад представляет собой простую команду для отстука на наш веб-сервер. Типичный метод Out of band (OOB). Плагин отображает, по какому из URL произошла обработка объекта и какой из запросов ее вызвал. Топорно, конечно, но это может сработать. Обычно для таких целей лучше использовать не внешний веб-сервер, а DNS-сервер, так как исходящие подключения часто заблокированы на файрволе, а вот DNS-туннель блокируют редко.

ПОЛУЧАЕМ RCE В SAML ЧЕРЕЗ XSLT

Мы уже рассматривали атаки с использованием XSLT, но все равно стоит напомнить, что это за технология. Она позволяет с помощью XSL-стиля поменять структуру XML. Но для нас XSLT интересен тем, что позволяет напрямую пихать код в стилях XSL, и этот код будет выполнен в ходе преобразования. В классическом случае проблема такой атаки в том, что чаще всего мы контролируем только сам XML-документ, но не XSL-стиль, по которому он будет преобразован. Однако на самом деле это не всегда так.

Есть ряд ситуаций, когда XSL-стиль может находиться прямо внутри самого XML. Да-да, в документе указывается описание того, как его необходимо преобразовать. Делается это за счет добавления в документ еще одного пространства **xmlns:xsl=http://www.w3.org/1999/XSL/Transform**. Предостерегаю тебя от того, чтобы пихать XSLT-вектор в каждый XML по аналогии с XXE. Поддержка XSLT на принимающей стороне (в XML-парсере) не повяжется просто так.

Увидеть, есть ли в браузере поддержка XSL внутри документов XML, мы можем при обработке файлов SVG, а также при использовании «глубоких» XML-технологий — таких как XML Digital Signature.

XML DSig используется для подписи XML-документов. Этот стандарт позволяет указывать XSLT-преобразования для документа до того, как будет проверена подпись. По идее, это было сделано для более гибкого взаимодействия. Когда есть разница между тем, как подпись считается на принимающей и на отправляющей стороне (разные кодировки, учет пробелов и лишних проблем — проблем возникает много), с помощью XSL-стиля можно компенсировать эту разницу. Для описания преобразования используется элемент Transform (в Transforms). Пример ты можешь увидеть на картинке.

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod
      Algorithm="http://www.w3.org/TR/2001/CR-xml-c14n-20010126">
    </ds:CanonicalizationMethod>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
    <ds:Reference URI="#Body">
      <!-- Start malicious XSLT transform -->
      <!-- ... -->
      <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116">
          <xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:java="java">
            <xsl:template match="/">
              <xsl:variable name="pwd:int" select="java:lang.Runtime" />
              <xsl:value-of select="$pwd:int/exec('/usr/bin/touch -c /tmp/pwned')" />
              <xsl:value-of select="$pwd:int/exec('/usr/bin/touch -c /tmp/pwned2')" />
            </xsl:template>
          </xsl:stylesheet>
        </ds:Transform>
      </ds:Transforms>
      <!-- End malicious XSLT transform -->
      <!-- ... -->
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>ZGZmMjMzMjIzNjIwNjFlMjFlMTRhZjNkMzRhNjNhNjNmZWNhNzNm</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
```

Подпись XML-документа с указанием трансформации

Получается, что у нас есть технология, которая из коробки поддерживает XSLT-трансформацию. Если видишь какой-то сервис, использующий XML DSig, значит, можешь попробовать заслать на него что-нибудь хорошее. При этом помни, что твой документ должен быть валидным и все элементы подписи тоже должны присутствовать. Сама суть может и не быть подходной, но она нужна, чтобы пройти первичный парсинг на корректность документа. А далее выполняется наши действия из стиля, и только после этого происходит проверка подписи.

Если вспомнить, где XML DSig используется постоянно, то на ум приходит Security Assertion Markup Language (SAML). Это такой открытый стандарт на базе XML, который используется для создания централизованной аутентификации и авторизации. Сам по себе он непрост, так что подробно разбирать его не будем. Важно, что он часто используется в крупных компаниях.

Что мы имеем в итоге? Есть протокол аутентификации SAML, в котором используется технология XML DSig, которая, в свою очередь, поддерживает XSLT-трансформацию. Эта длинная цепочка дает нам возможность до аутентификации получить RCE. Очень удобно! Конечно, в реальности все не всегда так просто: если разработчики или админы в курсе проблемы, то кастомные стили для XML DSig могут быть и отключены. ✖

Вадим Матвеев
Старший эксперт
по анализу данных
Positive Technologies
@vadimmatveev
vadim.matveev@
positive-ts.ru

WARNING

Все вредоносные сценарии/примеры носят чисто тестовый характер. Автор не несет ответственности за ущерб, нанесенный в результате использования данных сценариев/примеров. Все сценарии/примеры были проверены на работоспособность только в определенном окружении и могут не сработать в вашем случае. Все вредоносные сценарии/примеры предназначены для использования только в своей сети. Не пробуйте сканировать, взламывать, эксплуатировать уязвимости чужих сетей.

ОБЗОР ЭКСПЛОЙТОВ

АНАЛИЗ СВЕЖЕНЬКИХ УЯЗВИМОСТЕЙ

Сегодня мы разберем CSRF-уязвимость в популярном фреймворке phpBB, а также покажем пример поиска подобных ошибок в большом проекте. Дальше разберем свежую уязвимость MySQL и рассмотрим несколько, основанных на удаленном выполнении кода в Ruby on Rails.

CSRF-УЯЗВИМОСТЬ В PHPBB

CVE(s): нет
Дата релиза: 26 января 2016 года
Автор: Lander Brandt
CVSS: нет

Уязвимость была найдена в администраторской панели управления формы phpBB. Данная панель позволяет пользу BBCode добавлять смайлы, стили, глобальные анонсы/объявления, отслеживать новые/измененные/удаленные файлы, а также выполнять другие задачи.

Для выполнения любого из вышеуказанных действий администратору нужно лишь отправить соответствующий запрос, а для защиты от подделки запросов используется токен **phpbb_{hash}_{sid}**. Но, как он выяснился, когда пользователям создают со всеми правами, в том числе и на управление ботами, то для них не генерится CSRF-токен. Соответственно, с помощью ботов можно обойти проверку и выполнить любое из вышеуказанных действий. Для этого нужно, чтобы бот сделал начальный запрос на нужную страницу, а потом отправить нужный запрос.

Здесь сопровождение большинства параметров, использованных в вопросе, не. Часть из них берет свои значения из устаревшей функции **request_var()**, часть из **request_var()**, но с отсутствующим третьим параметром (**request_var(foo, bar)**), а часть из **request_var()** с третьим параметром, но некоторого исключительного с массивом. Массив этот является обязательным для ожидания, но если передать **1,2,0** (**1,2,0_POST**), то он не сломает такую ошибку. Так функция **trim()** и проверяется в начале типа:

Для того, чтобы не генерить лишнюю ошибку, нужно отправить запросы POST-ом. Кстати, так же можно сделать и для обходимости формы, а заменить на каждый CSRF-уязвимостью.

Для исправления уязвимости как добавлен CSRF-токен в phpBB. Показан пруф-о-уязвимости сделай на форме.

```
$ curl -b cookies.txt -c cookies.txt -d "action=add_ban&ban[0]=1"
```

Из названия функции **check_form_key()** ясно, что она проверяет токен CSRF, а если он неверный, то, соответственно, что делает это просто сравнивая значения. Ниже в файле есть такая вот строчка:

```
$ grep -Ir -A10 -B10 -n -e "check_form_key" *
```

То есть и добавление, и проверка токена CSRF осуществляется вручную. А это, в свою большую очередь, ведет к ошибкам.

Попробуем найти в исходниках вызовы функций **add_form_key()** и **check_form_key()** (вызовы создания и проверки токенов соответственно). Мы нашли, что **check_form_key()** на следующих сценариях показана результаты такого:

```
$ grep -Ir -A10 -B10 -n -e "add_form_key" *
```

Большинство комментов вызывает **check_form_key()**, но **add_form_key()** не вызывается нигде, кроме как в тестовых файлах, что можно использовать для. Мы же нашли, что в файлах, которые начинаются на **acp_**, вызывается **add_form_key()**. Для этого нужно, чтобы бот сделал запрос на страницу, а потом отправить нужный запрос.

Файл **acp_extensions.php** нам не слишком интересен, так как он всего лишь отображает шаблоны, а вот **acp_bots.php** нам интересен. Он отвечает за управление ботами и, соответственно, за их проверки обновлений. В виде исключения все операции такой CSRF уязвимости можно сделать, но, что интереснее, можно сделать так, чтобы бот сам отправлял на свои страницы.

А вот второй файл **acp_bbcode.php** подходит как нельзя лучше, так как отображает и обрабатывает POST-ом. Но, в отличие от **acp_bots.php**, в нем вызывается **add_form_key()** для генерации формы. В итоге, в итоге, получается CSRF токен, мы можем создавать произвольные комнаты BBCode через бот.

Есть только одна проблема: можно генерить и ошибку, что не слишком хорошо. Но, в принципе, phpBB поддержу дополнительных сценариев, которые, по-видимому, не. Поэтому, если бот сделает запрос на страницу, то, если не делает на какие-нибудь вызов ошибки, то можно, и, в принципе, сделать.

Если, конечно, не считать то, что есть на проектировщиков пользователя, проекта **phpbb.com**, которые, в принципе, не. Поэтому, что, если, если перед ними, то, даже несмотря на проектировщиков? Тогда мы получим вариант, когда? Поэтому, Почему проектировщики не сделали на Ruby on Rails?

```
$ grep -Ir -A10 -B10 -n -e "check_form_key" *
```

Вот как бы выглядеть результат работы:

```
/var/www/forum/ucp/ucp_notifications.inc:
-rw-r--r-- 1 root root 2 Jan 26 10:00 .
drwxr-xr-x 1 root root 4 Jan 26 10:00 ..
drwxr-xr-x 1 root root 4
```

СОВРЕМЕННЫЙ ХЕШРЕКИНГ

ВЗГЛЯД НА ВЗЛОМ ХЕШЕЙ ИЗНУТРИ

Дмитрий Дмитриев
Эксперт по информационной безопасности

Часто хакер предпочитает огромную работу для промежуточного взлома, а потом, уже получив в руки полезную добычу, спокойно отдыхает долгое время — подбор паролей к хешам, которые, в отличие от паролей, не обновляются годами, занимает не одну неделю. На сложные пароли уходят месяцы, а на простые — до 10 минут, но иногда и очень, чтобы успешно воспользоваться даже самым слабым паролем, нужно 4 месяца! Сегодня существует и такое, что профессионалы занимаются взломом паролей многие годы!

ЧТО ТАКОЕ ХЕШИРОВАНИЕ?

Если коротко, то хеширование — это, как мешалка (от англ. hash: смешать, — мешать, размешивать, вещать), для которого требуется исходная информация, которая, в результате, перемешивания, выдает уникальный результат, который, в отличие от мешалки, не может быть обратно разделен на исходные ингредиенты. Высокоэффективность работы сервера в течение многих недель и месяцев при хешировании паролей.

Итак, если исходной информацией является пароль, то хеширование — это алгоритмы, которые в сочетании с генератором чисел для случайных значений, — «соль», — выдают уникальный результат, который, в отличие от пароля, не может быть обратно расшифрован. Но, если знать пароль, то можно, на основе соли, сделать то же самое, и, если результаты, не только совпадают, но и равны, то пароль, — верный. Для чего нужно хеширование? Для того, чтобы, в случае, если злоумышленник, получит, к примеру, базу данных, с паролями, то, для того, чтобы, использовать, пароли, нужно, сначала, подобрать, соль, и, только, после, этого, можно, приступать, к, подбору, паролей, — это, в, разы, сложнее, чем, просто, подобрать, пароли, для, которых, не, нужно, использовать, соль. Для чего нужно использовать соль? Для того, чтобы, не, использовать, одинаковые, пароли, для, разных, пользователей, — если, пароли, одинаковые, то, злоумышленник, сможет, подобрать, пароль, для, одного, пользователя, и, использовать, его, для, всех, остальных, пользователей, — если, пароли, разные, то, злоумышленник, сможет, подобрать, пароль, для, каждого, пользователя, — в, случае, если, пароли, одинаковые, — для, ускорения, подбора, паролей, — для, получения, максимальной эффективности, — необходимо, использовать, — одинаковые, — пароли, — для, — разных, — пользователей.

Для работы на GPU приложения также, в большинстве, случаев, используют, технологии, — CUDA, — и, — OpenCL, — — CUDA, — технология, — компании, — NVIDIA, — — OpenCL, — технология, — компании, — Apple, — — CUDA, — технологии, — компании, — NVIDIA, — — OpenCL, — технологии

THERE IS NO 100% GUARANTEE

Юрий Гольцев
@yggotsev

Тестирование на проникновение (penetration testing) — метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника. Для кого-то это хобби, для кого-то работа, для кого-то это стиль жизни. На страницах нашего журнала мы постараемся познакомить тебя с профессией настоящего хакера на службе корпорации, с задачами, которые перед ним ставятся, и их решениями.

INTRO

Когда кто-нибудь пытается убедить меня в том, что он, компания или продукт способны выявить абсолютно все уязвимости в тестируемой системе, я могу лишь предположить, что передо мной либо кто-то из отдела продаж, либо некомпетентный технический специалист. С увеличением скоупа количество векторов атак растет в геометрической прогрессии (FUD! Deal with it!).

В идеальном мире это должен понимать как исполнитель, так и заказчик. Как ты знаешь, мы в таком мире не живем. Каждый уважающий себя и своего заказчика консалтер перед заключением договора тщательно обговаривает нюансы и возможные спорные моменты. Заказчик должен знать, почему подобные работы не дают спорщикам раскрытия всех уязвимостей ИС. Это аксиома. Количество найденных уязвимостей напрямую зависит от их наличия и от компетенции исполнителя. В общем случае консалтер обязуется применить предложенную методологию поиска определенных типов уязвимостей в отношении обозначенного перечня ресурсов. То, что в результате работ по оценке анализа защищенности доказуется новые техники эксплуатации и векторы атак, — явление побочное и абсолютно не обязательное.

ПРЕЦЕДЕНТ

В январе 2016 года произошел интересный и первый в своем роде прецедент: на компанию, которая занимается консалтингом в сфере ИБ, был подан иск в суд. Причина — заказчик, изучив отчет о проделанной работе, заподозрил исполнителя в отсутствии технических компетенций.

История началась в октябре 2013 года. Некая организация Affinity Gaming, которая занималась игорным бизнесом, обнаружила утечку данных кредитных карт своих клиентов. В рамках разрешения владельцы казино заключили контракт с фирмой Trustwave, которая обязалась провести расследование инцидента и, вероятно, дать рекомендации по устранению уязвимостей.

По словам представителей Trustwave, заказчик был уведомлен о том, что «качество услуг, предоставляемых в рамках их соглашения, полностью сопоставимо с качеством аналогичных услуг, оказываемых другими компаниями, являющимися признанными профессионалами в области ИБ». По окончании работ сотрудники Trustwave заверили заказчика в том, что источник утечки обезврежен. Я предполагаю, что было проведено как минимум расследование инцидента (выявление вектора, хронология действия атакующего). После чего на основании этих данных скомпрометированная ИС, скорее всего, была «вычищена» (установлены заплатки, изменены пароли, удалены бэкдоры и так далее).

Далее произошло вот что. Для соответствия очередному стандарту, который формировал игорный комитет штата Миссури (где расположен такой казино Affinity), необходимо было провести тестирование на проникновение. В апреле 2014 года руководство Affinity Gaming обратилось за этой услугой в небезызвестную компанию Ernst & Young. Аудиторы E&Y обнаружили в сети подозрительную активность, источником которой, как выяснилось, была программа Metasploit exe. Важный момент: этот самый бэкдоринг был исследован Trustwave, но его сомнительные функции не были упомянуты в отчете.

Казалось бы, такое случается: между аудитами прошло некоторое время, состояние ИС могло измениться. В параграфе PRELIMINARY STATEMENT иска не сказано, каким образом было выявлено, что отчет Trustwave — полная туфта. Этот момент поставил под вопрос все результаты работы Trustwave.

Владелец казино обратился в IT-security компанию — Mandiant. Ребята из этой конторы провели собственное расследование и в итоге пришли к выводу, что отчет Trustwave был очень неточным, и складывалось впечатление, что работы были проведены невыразительно. По факту Trustwave солгал заказчику о том, что источник утечки данных был диагностирован и устранен. В реальности исполнитель изучил лишь малую долю ресурсов и так и не смог точно выявить, как именно было осуществлено проникновение.

Заказчик в результате посчитал, что договор грубо нарушен и Affinity понесла колоссальные убытки, в связи с чем неплохо было бы, если бы исполнитель вернул все потери. В Trustwave делать это отказались, и в результате в конце 2015 года компания Affinity Gaming подала иск в суд.

Вероятно, если бы не иск, эта история не стала бы достоянием общественности. Неудивительно, что в Trustwave с иском не согласны: компания пытается отстоять в суде свою репутацию. К сожалению, какие-либо технические детали этого события остаются пока за кадром, так что судить о том, что именно произошло и кто прав, не представляется возможным.

PIECE FROM MY REALITY

В моей практике была относительно похожая история. Для одной крупной компании был проведен комплексный тест на проникновение. Как и в большинстве случаев, проникновение было осуществлено извне и был получен полный контроль над всеми системами заказчика. Отчет был подготовлен и передан представителям компании, проведена презентация результатов для руководства. Все довольны, договор закрыт.

По завершении проекта я имею привычку забывать большинство технических деталей проведенных работ, а через какое-то время и сами заказчики забывают. Я считаю эту особенность даже полезной, голова не забивается бесполезной информацией. В этот раз быстро забыть детали проекта не получилось.

Спустя месяц после сдачи отчета, листая ленту твиттера, я наткнулся на твит, содержащий информацию об уязвимости на одном из ресурсов моего заказчика. Прилагались и логи ее эксплуатации. Из этого pwnage было понятно, что уязвимость в ресурсе была очевидной. Если честно, в этот момент мне стало немного не по себе — технические детали работ начали забываться, и я не был уверен в том, что нашел эту уязвимость и рассмотрел в отчете.

Признаюсь честно, я перешел в режим паранойи: а вдруг о себе и о том, какой удар подобное событие может нанести по ЧСВ и репутации. В течение трех месяцев после окончания работ у меня хранится зашифрованный архив проектных данных — на случай если заказчику понадобится дополнительная консультация или бэкап результатов. В нем я нашел описание уязвимости, которая стала достоянием общественности. С одной стороны, ЧСВ и репутация спасены, а с другой стороны, взломанный ресурс оказался одной из точек проникновения во внутреннюю сеть заказчика.

Я начал серьезно переживать за отдел ИБ заказчика и эту компанию в целом. Я решил уведомить отдел ИБ о том, что есть некоторая вероятность того, что их система была скомпрометирована кем-то со стороны. Я ограничился небольшим почтовым сообщением, где изложил мои подозрения, и ссылкой на источник.

Из любопытства и желания помочь безопасникам я принялся изучать логи pwnage. В этот момент я осознал, что, скорее всего, мои волнения были напрасными. После анализа доказательств взлома, выложенных на публике, стало понятно, что весь инцидент — проделки скрипт-кидди с sqlmap в консоли.

Ставка была сделана на то, что уязвимый ресурс доступен на одном из доменов серверной транснациональной корпорации. Соответственно, публикация подобного pwnage будет сконвертирована людьми, далекими от ИТ и ИБ, в популярность героя, который так и остался неизвестен. «Хакер», вероятно, даже не понял, куда он попал и какие это перед ним открывает возможности в плане развития атаки. Он решил ограничиться лишь беспоясным дампом БД, даже не удосужившись немного изучить код приложения и добиться RCE.

Я передал свои предположения и выводы представителю заказчика. По результатам внутреннего расследования мои выводы подтвердились. Вес голоса отдела ИБ значительно вырос, что позволило им проверить мероприятия по устранению найденных уязвимостей в кратчайшие сроки.

Как видишь, эта история для всех завершилась хорошо. Я не уверен, что, если бы в моем отчете отсутствовала информация об этой уязвимости, заказчик подал бы на меня в суд. Но, так или иначе, если бы уязвимость была пропущена по моей вине, меня бы мучила совесть. В таком случае следовало бы как минимум устранить причину подобной ошибки на моей стороне и безоговорочно компенсировать трудозатраты по расследованию инцидента безопасности. Ну и конечно, принять в нем активное участие.

ВЫВОДЫ

Делать какие-то конкретные выводы относительно истории с Trustwave пока рано, посмотрим, как события будут развиваться дальше. Побываав в роли заказчика случаев тестирования на проникновение хотя бы пару раз (и работая с разными компаниями), понимаешь что «пропустить» одну уязвимость, но найти другую — совершенно обычная ситуация для любого исполнителя. Глупо это отрицать.

Я считаю, что это объяснимо — все сильно зависит от обговоренного скоупа, сроков выполнения работ и состава команды исполнителя. Ситуация становится печальной, когда разница в результатах работ при относительно одинаковых исходных данных колоссальна. На мой взгляд, обеим сторонам стоит форсировать добавление в договор дополнительного пункта: об ответственности сторон.

К примеру, в случае возникновения обоснованных сомнений со стороны заказчика в компетенции исполнителя и результатах проведенных им работ заказчик вправе обратиться в третью организацию для проведения аналогичных работ. В том случае, если результат работ, проведенных третьей организацией, окажется более компетентным, недобросовестный исполнитель обязуется компенсировать издержки заказчика.

Немного уточнимо — сработает разве что в идеальном мире. Но если в договоре есть информация о методологии тестирования (а также перечне тестируемых ресурсов и прочем), то исполнитель как минимум будет гарантировать, что заказчик получит ожидаемый результат. Добросовестному и компетентному исполнителю такой пункт нестрашен, а вот заказчика он может защитить от недобросовестного и некомпетентного.

Сложно будет только выбрать третью независимую организацию для проведения проверки. Помимо этого, заказчику стоит отстраниться от полного аутсорса технических компетенций. Обязаться ими стоит хотя бы ради того, чтобы понять, насколько некомпетентной может показаться компания-исполнитель. Что же касается исполнителя, то следует постоянно совершенствовать технические компетенции, развиваться, следить за тенденциями как offensive-, так и defensive-индустрии.

OUTRO

История с Trustwave очень интересна с точки зрения взаимоотношений заказчик — исполнитель в индустрии ИБ. Из-за отсутствия технических данных и полных обоснований в публичном доступе нет смысла кого-то обвинять или защищать. Остается только следить за развитием событий — возможно, этот прецедент станет причиной появления чего-то нового в индустрии ИБ-консалтинга. К чему бы это нас это ни привело, делай свое дело так, чтобы тебе никогда не было стыдно за результат. Stay tuned! ⌶

ПОЛЕЗНАЯ ИНФОРМАЦИЯ

Общая теория по пентестам

- Vulnerability Assessment
- Open Source Security Testing Methodology Manual
- The Penetration Testing Execution Standard

Немного практики

- PentesterLab
- Penetration Testing Practice Lab

В закладки

- Open Penetration Testing Bookmarks Collection

Right way to contribute

- DC7862
- DC7812
- 2600 russian group

→

ВЛОГ

ПРОКАЧАЙ СВОЙ NMAP

РАСШИРЯЕМ ВОЗМОЖНОСТИ ЮНИТЕЛЬНОГО СКАНЕРА ПОРТОВ С ПОМОЩЬЮ ПОЛЬЗОВАТЕЛЬСКИХ СКРИПТОВ

Дмитрий Евдокимов
Digital Security

Nmap — культовый сканер, без которого не может обойтись практически ни один хакер, поэтому тему расширения его возможностей мы уже поднимали. Но в прошлом обзоре мы лишь пользовались в Nmap другим инструментом — сборкой Zenmap. В статье ребята подготовили тоже, но на сей раз рассмотрим, как расширять возможности Nmap с помощью любимого инструмента. Зорбоксов не нажать, сразу кнутку и погнали.

Nmap — это не просто сканер портов, а полноценный инструмент для исследования и диагностики. Использование скрипта в Nmap может помочь хакерам более автоматизированно взламывать системы, а сисадмину — ускорить проверку. Nmap — это не просто сканер портов, а сканер-мечта.

ПАРА СЛОВ ОБО ВСЕМ

Напомню, что пользователи человеческих языков — вместо ответа на вопрос «Как вы?» — обычно спрашивают «Как поживаете?». Так вот, Nmap — это не просто «как вы», а «как поживаете» сетевой инфраструктуры. Он может ответить на вопросы, какие порты открыты, на какие из них не брошены, с каким ПО они работают, какие версии ПО на них запущены, есть ли на них ошибки, не брошены ли они, не заблокированы ли они, сколько времени ушло на ответ, сколько пакетов потерялось, какие ОС и версии ОС на них запущены, какие версии ядра на них запущены, какие версии Linux на них запущены, какие версии Windows на них запущены, какие версии Linux на них запущены, какие версии Windows на них запущены, какие версии Linux на них запущены, какие версии Windows

Дмитрий «0ig1» Евдокимов,
Digital Security
@evdokimovds

X-TOOLS

СОФТ ДЛЯ ВЗЛОМА И АНАЛИЗА БЕЗОПАСНОСТИ

WARNING

Внимание! Информация предназначена исключительно с целью ознакомления! Не редакция за твои действия ответственности не несут!

POWER OF COMMUNITY 2015: ФИНГЕРПРИНТИНГ СМАРТФОНОВ

Денис Макрушин
defec.ru, twitter.com/dfeuza

Power of Community — южнокорейская конференция по практической информационной безопасности, где вот уже с 2006 года собирается преимущественно корейская и китайская аудитория. Несмотря на кажущуюся «местечковость», программа мероприятия пестрит докладами спикеров из разных стран, чьи имена часто встречаются на более крупных конференциях.

В Сеуле меня ждало много интересного и эксклюзивного контента от местных спикеров, много общения и веселый CTF, построенный по принципу «сделай таски и дай решить их другим». Кстати, в этом году на соревнованиях Россию представляла команда, название которой ты сможешь угадать с одной попытки, взглянув на первую фотографию, где ребята вежливо «заменили» scoreboard на свою картинку.

Попробуй угадать, какая российская команда посетила PoC в этом году

The Grugq открывает первый день докладом о развитии APT и концепции clicking-clicking war

ОТ «ОТПЕЧАТКА» АКСЕЛЕРОМЕТРА ДО ГЛОБАЛЬНОЙ CLICKING WAR

Двухдневная программа конференции началась с вступительного слова организатора. Увы, но уловить что-либо об исторических особенностях развития PoC, о его целях и подводных камнях его организации не получилось, потому что обращение было адресовано корейской аудитории. Однако после общения тет-а-тет с организаторами стала понятна цель: популяризовать индустрию среди молодого поколения. Другими словами: евангелизм и организация комьюнити.

Фактически ключевым докладом, который открывает мероприятие, стала презентация от The Grugq. С этим псевдонимом плотно ассоциируются теги «эксплоит», «брокер», «0day». Однако в этот раз The Grugq углубился в актуальную нынче тему APT, попытался предсказать варианты развития таргетированных атак в обозримом будущем и описал сценарий так называемых clicking-clicking wars — третьей мировой войны, где каждый солдат не держит ничего тяжелее мышки, но при этом она может стать страшным оружием в его руках.

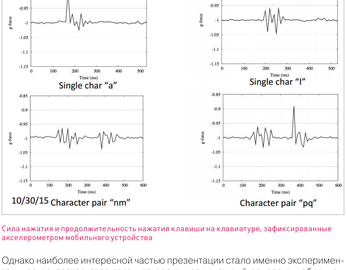
Доклад от Сюй Вэньюань (Wenyuan Xu), научной сотрудницы Чжецзянского университета (Zhejiang University), рассказывающий о том, как всевозможные сенсоры в мобильном телефоне могут упростить задачу трекинга его пользователя и однозначно идентифицировать его устройство среди других, был подкреплен не только глубокими теоретическими обоснованиями, но и практическими результатами. Сюй Вэньюань выделила категории сенсоров, которые тем или иным образом могут что-то рассказать об устройстве:

- определение положения устройства;
- определение жестов пользователя;
- определение местоположения;
- компас;
- взаимодействие с другими устройствами.

Каждая из категорий обладает конкретными технологическими представителями (Wi-Fi, NFC, гироскоп, GPS, датчик температуры и прочее). В свою очередь, каждый из них служит потенциальным источником для получения уникального «отпечатка» устройства (device fingerprinting).

Сюй Вэньюань рассказывает о «недокументированных» особенностях акселерометра в твоем мобильном устройстве

Кроме того, имеющиеся сенсоры, как известно, могут стать дополнительным каналом утечки информации — Сюй Вэньюань еще раз экспериментально это подтвердила. На размещенном неподалеку от клавиатуры мобильном устройстве акселерометр зафиксировал характеристики нажатия клавиш. В процессе дальнейшего исследования полученных данных госпожа Сюй Вэньюань еще раз подтвердила, что данные характеристики уникальны.



Сила нажатия и продолжительность нажатия клавиши на клавиатуре, зафиксированные акселерометром мобильного устройства

Однако наиболее интересной частью презентации стало именно экспериментальное доказательство того, что практически каждый сенсор в мобильном устройстве может идентифицировать пользователя по нескольким параметрам: уникальный фингерпринт самого сенсора, который появляется в результате особенностей его производства и особенностей его применения самим пользователем (наличие определенных приложений в телефоне, езда в машине с мобильником на соседнем сиденье или в «бардачке», захват вибраций от мотора и так далее). С деталями исследования рекомендую ознакомиться в подробном райтапе. Электронные паспорта, биочипы и прочие попытки «пометить» человека для того, чтобы однозначно идентифицировать его онлайн, — все это лишь формальные процедуры. На самом деле весь твой телефон — это самый настоящий электронный паспорт, который позволяет отличить тебя от сотни тысяч других владельцев подобного девайса.

Элементарные микроотклонения в физических параметрах компонентов акселерометра, которые образуются в результате «неидеальности» производственных процессов, рождают уникальные особенности полученного в результате девайса. И если кому-то покажется, что нет особого смысла в фингерпринтинге мобильных юзеров, то этот кто-то заблуждается.

Уже сейчас рекламные агентства и разработчики мобильных приложений и приложений для «носимой электроники» ведут охоту за твоими привычками и поведением в онлайне: какие ресурсы ты посещаешь, в какое время суток ты наиболее активен, а в какое время ты склонен делать дорогостоящие покупки, где ты любишь ужинать со своим партнером и многое другое. Только они накапливают эту статистику не с помощью кукис-файлов твоего браузера, которые ты периодически удаляешь всевозможными клинерами, а посредством различных вспомогательных технологий фингерпринтинга. В данном случае сенсоры твоего мобильного устройства как нельзя лучше подходят для задач твоей идентификации среди тысяч других посетителей твоего любимого кафе, у которых точно такая же модель телефона, как и у тебя.

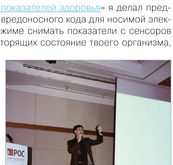
Если также допустить тот факт, что фингерпринт не передается сам по себе, а ему сопутствует различная полезная информация вроде истории посещений, показателей активности, GPS-координат, то становится немного не по себе. Например, страховые агентства, обладающие информацией о том, что ты любишь скоростную езду и частенько посещаешь бары, могут увеличить стоимость страховки твоего авто без объяснения причин.

Ключевые этапы процесса фингерпринтинга

В своем материале «Угрозы трекинга показателей здоровья» я делал предположение о появлении специального вредоносного кода для носимой электроники, который будет в фоновом режиме снимать показатели с сенсоров устройства, прямо или косвенно мониторящих состояние твоего организма, и отправлять эти данные третьей стороне. Уникальный фингерпринт сенсоров может стать отличным дополнением к данной информации.

И НЕ НУЖЕН ЗАНАВЕС ЖЕЛЕЗНЫЙ

Интересное наблюдение: региональная специфика часто не выползает за пределы своих территорий и без всяких запретительных инициатив со стороны государства. Это касается и исследований в сфере информационной безопасности: достаточно большое число толковых ресерчей остаются опубликованными в пределах одной территории и, увы, не слышны на громких мейнстримовых конференциях. Этим и примечательны небольшие региональные конференции с «местной» спецификой и с местным образом мыслей, который приводит к уникальным результатам.



Opppa... Gangnam style

→

БЕСПЛАТНЫЕ АНТИВИРУСЫ — ПРОВЕРКА БОЕМ

Сергей Кулешов
ПРОГРАММИСТ

НАСКОЛЬКО ХОРОШИ БЕСПЛАТНЫЕ АНТИВИРУСЫ ЛУЧШИМ ОТ ПЛАТНЫХ? ПРОВЕРИЛИ ЭКСПЕРТЫ «ЛАБОРАТОРИИ КАСПЕРСКОГО».

Многие разработчики защитных программ выпускают бесплатные антивирусы. В этом году даже ЗАО «Лаборатория Касперского» выпустила бесплатный антивирус Kaspersky Free. Насколько базовые функции (достаточные для предотвращения заражения в реальных условиях — например, при веб-серфинге? Чем платные версии отличаются за бесплатный сыр? Давай выясним это.

МЕТОДИКА ТЕСТИРОВАНИЯ

Для тестирования использовались обновленные версии последних релизов. Сразу отмечу, что в тестах участвовали только «чистые» версии — ни одна из них не была «заточена» под конкретный тест. Все антивирусы были установлены с настройками по умолчанию. Затем на первом операционном системе (Windows 7 Ultimate x64 SP1) с помощью Wyse PC Agent и Wyse Rapport перейдя сделан снимок. Потом, запустив в ней Wyse PC Agent и Wyse Rapport, Kaspersky Free, AVG и Avira Free Antivirus, мы сделали еще по одному снимку. Затем в каждой из этих ОС мы установили по одному из антивирусов и сделали еще по одному снимку. Таким образом, мы получили по пять снимков для каждого антивируса.

KASPERSKY FREE

Размер дистрибутива 16.5 Мб, установленного — 147,8 Мбайт. После установки и обновления Kaspersky Free занимает на диске 232 Мбайт. Он обладает всеми функциями, которые есть в платных версиях, но в отличие от последних, полностью отключены функции контроля приложений и контроля сетевой активности. Дополнительные функции отключены изначально — это сделано для облегчения жизни новичкам Kaspersky Free.

Окно Kaspersky Free

Kaspersky Free обнаруживает другую и перемещает файл в карантин

В нашем тесте Kaspersky Free не пропустил ни одной вредоносной угрозы. Часть из них он обнаружил сразу, часть — при попытке запуска, часть — при попытке записи на жесткий диск. Интересно, что ни одна из вредоносных программ,

Kaspersky Free обнаруживает сомнительный запуск программы, которая могла нанести ущерб системе

Kaspersky Free обнаружил сомнительный запуск программы, которая могла нанести ущерб системе

Kaspersky Free обнаружил сомнительный запуск программы, которая могла нанести ущерб системе

Kaspersky Free обнаружил сомнительный запуск программы, которая могла нанести ущерб системе

Kaspersky Free обнаружил сомнительный запуск программы, которая могла нанести ущерб системе

Kaspersky Free обнаружил сомнительный запуск программы, которая могла нанести ущерб системе

AVIRA FREE ANTIVIRUS 2014

Размер дистрибутива 1,1 Гб. Для установки необходимо фиксированность и добавлено выполнение для каждого из компонентов. Размер дистрибутива Avira Free Antivirus 2014 занимает на диске 1,1 Гб. Для установки ещё на время установки ещё занимает 1,1 Гб. Для установки ещё на время установки ещё занимает 1,1 Гб. Для установки ещё на время установки ещё занимает

Начало статьи

БЕСПЛАТНЫЕ АНТИВИРУСЫ — ПРОВЕРКА БОЕМ

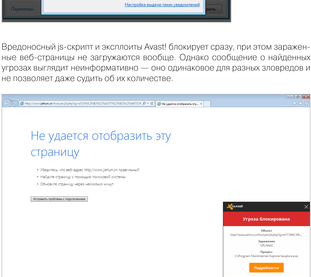
НАСКОЛЬКО ХОРОШИ БЕСПЛАТНЫЕ АНТИВИРУСЫ И ПОЧЕМУ ОНИ БЕСПЛАТНЫ?

AVAST! FREE ANTIVIRUS (11.1.2245)

При установке Avast! также надо быть внимательным: по умолчанию отмечена установка Google Chrome и Google Toolbar для IE. После установки без дополнительных компонентов антивирус занимает 604 Мбайт — много, но вдвое меньше Avira Free.

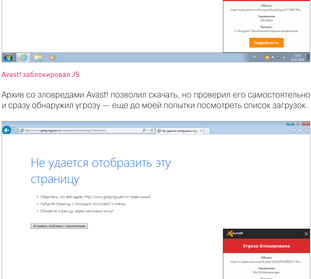
Скрытой рекламы полно даже в главном окне антивируса. Обещанный подарок оказывается формальной скидкой на платные продукты. На вкладке «Инструменты» указаны не необходимые модули защиты, а рекламные ссылки на их описание. Стоит кликнуть одну из них, как предложение выбрать вариант дополнительной платной защиты надолго поселится в главном окне Avast.

При попытке вручную запустить заблокированный MSS экземпляр со стороны Avast! не встречаем никакого сопротивления. Потенциально опасный файл (даунлоадер) с недействительной подписью игнорируется антивирусом.



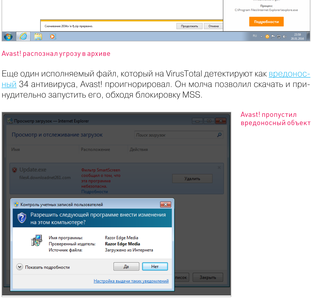
Avast! не считает файл опасным, и зря

Вредоносный js-скрипт и эксплоиты Avast! блокирует сразу, при этом зараженные веб-страницы не загружаются вообще. Однако сообщение о найденных угрозах выглядит неинформативно — оно одинаковое для разных зловредов и не позволяет даже судить об их количестве.



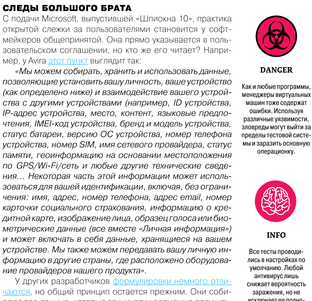
Avast! заблокировал JS

Архив со зловредами Avast! позволил скачать, но проверил его самостоятельно и сразу обнаружил угрозу — еще до моей попытки посмотреть список загрузок.



Avast! распознал угрозу в архиве

Еще один исполняемый файл, который на VirusTotal детектируют как вредоносный 34 антивируса, Avast! проигнорировал. Он молча позволил скачать и принудительно запустить его, обходя блокировку MSS.



Avast! пропустил вредоносный объект

СЛЕДЫ БОЛЬШОГО БРАТА

С появлением Microsoft, выпустившей «Шлюзовка 10», практика открытой слежки за пользователями становится у софтмейкеров общепринятой. Она прямо указывается в пользовательском соглашении, но кто же его читает? Например, у Avira этот пункт выглядит так:

«Мы можем собирать, хранить и использовать данные, позволяющие установить вашу личность, ваше устройство (как определено ниже) и взаимодействие вашего устройства с другими устройствами (например, ID устройства, IP-адрес устройства, место, контент, языковые предпочтения, IMEI-код устройства, бренд и модель устройства, статус батареи, версию ОС устройства, номер телефона устройства, номер SIM, имя сетевого провайдера, статус памяти, геоинформацию на основании местоположения по GPS/Wi-Fi/сеть и любые другие технические сведения... Некоторая часть этой информации может использоваться для вашей идентификации, включая, без ограничения: имя, адрес, номер телефона, адрес email, номер карточки социального страхования, информацию о кредитной карте, изображение лица, образец голоса или биометрические данные (все вместе «Личная информация») и может включать в себя данные, хранящиеся на вашем устройстве. Мы также можем передавать вашу личную информацию в другие страны, где расположено оборудование провайдеров нашего продукта».

У других разработчиков формулировки немного отличаются, но общий принцип остается прежним. Они собирают все данные, которые технически возможно получить. Поскольку антивирус глубоко интегрируется в ОС, устанавливает собственные драйверы и перехватывает системные вызовы, он имеет доступ ко всей информации — в том числе зашифрованной, поскольку ее хотя бы раз расшифровывал сам пользователь.

На этом фоне обнадеживает заявление Евгения Касперского, которое он сделал, анонсируя выпуск бесплатного антивируса имени себя: *«Он будет построен на тех же технологиях, что и платные персональные продукты... Без слежки за пользователем в рекламных целях и торговли его конфиденциальностью. Никакой такой фигни — только из-за защиты»*, — писал он в ЖЖ.

Впрочем, и здесь не обходится без доли лукавства. Сам Kaspersky Free собирает только общую обезличенную статистику, вроде количества найденных угроз по их типам. Однако в нем по умолчанию включен облачный сервис Kaspersky Security Network, в KSN известен своими аппетитами к сбору информации. В него отправляются подробные логи, которые включают список установленных программ вместе с путями, детальный мониторинг работы пользователя, списки запущенных процессов, статистику использования приложений и другие приватные данные. Отключить его можно на соответствующей вкладке.

Тайный агент KSN

ВЫВОДЫ

Как видно из этого небольшого эксперимента, все антивирусы реагировали на один и те же угрозы немного по-разному. Один блокировал переход по ссылке, отобразив предупреждение на панном стране. Другие не дали скачать зараженный файл или предотвратили запуск вредоносного скрипта, а третьи среагировали только на локальный запуск зловреда или вообще пропустили его. Дело здесь не в том, что платный антивирус лучше бесплатного от того же разработчика — у них одинаковый движок и базы. Просто в платных версиях используются дополнительные модули защиты, благодаря которым угрозы распознаются и блокируются не только по сигнатурному анализу.

Kaspersky Free в целом не вызвал существенных нареканий. Он очень похож на урезанный KIS, из которого убрали опциональные компоненты и защиту от дурака, добавив рекламы и спрятав поглубже KSN.

Avira отличилась чудовищно долгой установкой и проворливостью. Она занимала больше всех места, а компьютер с ней ощутимо тормозил на элементарных операциях. С архивами она практически не работает. Во всяком случае, не проверяет скачанные из интернета до их ручной распаковки.

Avast! проигнорировал пару серьезных угроз (пользователю хватит и одной) и тоже изобилует хитрой рекламой. Обнадеживаемые зловреды он блокирует сразу, но понять, что произошло, без детального анализа лога невозможно. Сообщения антивируса выглядят одинотично и не подразумевают выбора со стороны пользователя — обычно это просто уведомления о принятом решении.

AVG в целом выглядит адекватно, однако политика компании в отношении данных пользователя оставляет желать лучшего. Если бы не ультиматум о сборе сведений, его можно было бы рекомендовать как неплохой бесплатный антивирус.

DANGER

Как и любые программы, менеджеры виртуальных машин тоже содержат ошибки. Используя различные уязвимости, зловреды могут выйти за пределы тестовой системы и заразить основную операционку.

INFO

Все тесты проводились в настройках по умолчанию. Любой антивирус лишь снижает вероятность заражения, но не исключает ее полностью. Для повышения безопасности следует использовать более агрессивные настройки и дополнительные инструменты — файрвол, средства проактивной защиты, изоляция потенциально опасного кода, антиэксплоит и другие. В платных антивирусах большинство из них уже интегрировано, однако при желании можно самостоятельно сделать подобный набор из бесплатных утилит.

WWW

Kaspersky Free

Avira Free Antivirus 2016

AVG AntiVirus FREE

Avast! Free Antivirus

WARNING

Все тесты выполнялись только в исследовательских целях. Необходимые файлы были загружены с общедоступных ресурсов. Разработчики протестированных антивирусов получили автоматические уведомления о результатах сканирования. Редакция и автор не несут ответственности за любой возможный вред.

КОДИНГ

ЧЕРНАЯ МАГИЯ GIT HOOK

КАК НЕ ПУСТИТЬ ДЖУНИОРОВ В МАСТЕР-ВЕТКУ И ВООБЩЕ ВСЕ АВТОМАТИЗИРОВАТЬ

Ринат Абдуллин, Рыбинский УАТК
rinat.a.ru@gmail.com

При code review ты указываешь разработчикам на забытый **printf**, **console.log**? Сумасшедшие коды с синтаксической ошибкой? Или хочешь разграничить права на работу в ветвках, но боишься, потому что джуниор пушит порядок веток при слиянии? Хватит это терпеть! Учас же есть Git и Bash!

ЛЕГКИЙ СТАРТ С GIT HOOKS

Git поставляется с несколькими примерами **хуков** — скриптов-callback'и, запускаемые git, когда произходит определенное действие. В частотном списке это наверняка Dreamer и Gitx.

В качестве действия может выступать **commit apply patch merge push rebase** и другие операции. Мы можемداемит, что мы можем использовать только для проверки формата сообщений коммита, но их область применения гораздо шире. Например, можно запрещать пушить в определенные ветки, можно запускать git, что работает внутри **SPROJECT_DIR/.git/hooks/**. Изменения в этой директории не может быть закоммичено и распространено между членами команды. Также нам можно импортировать, используя дополнительный флаг **git clonit --template=**.

- Серверные — хуки, исполняемые уходят где-то. Они будут применяться на всем репозитории сервера.
- Для установки такого хука также достаточно изменить файл в директории **SPROJECT_DIR/.git/hooks/**, но делать это нужно в удаленном репозитории. Пересмотр использования таких хуков нельзя. Также при клонировании репозитория не получишь такие хуки, они остаются на удаленном репозитории.

Писать Git hooks можно на любом скриптовом языке: Python, PHP, Ruby, PowerShell или Perl. Я буду писать будет использовать Bash.

Мой ускоряющий с результатом скорого выполнения с помощью кода кодировать, или перешедшие на Windows, начиная от 8.0, то исполнения скриптов и использовать утилиты **git commit.git push** и так далее) не получится.

Встроенный хук

При создании репозитория команда **git init** также создается примеры хук-файлов, которые можно использовать в дальнейшем.

```
$ capsim@jolly-roger:/PDRV.git/hooks ls
applypatch-msg.sample  post-update.sample  pre-commit.sample
commit-msg.sample      pre-applypatch.sample  pre-push.sample
pre-rebase.sample      pre-receive.sample  prepare-commit-msg.sample
```

Для того чтобы начать их использовать, достаточно скопировать интересующий файл, убрав расширение: запрещ **pre-commit.sample** **pre-commit**, и убедиться, что для него выставлены права на исполнение, если нет — выполнить **chmod +x pre-commit**

ХУК СЛЕЖЕ, ХУК СПРАВА

Теперь перейдем к делу. Самое время попрактиковаться на реальных примерах.

Запрет на push в ветку

Начнем с простого. Допустим, у нас назначили pre-receive, который исполняется перед тем, как в удаленном репозитории произойдет изменение. Нам нужно запретить push. Если хук это дает код ошибки, отличный от 0, то исполнение прекратится и запрещенное изменение не произойдет.

Предположим, мы создаем ветку **pre-commit**, и убедимся, что для него выставлены права на исполнение, если нет — выполняем **chmod +x pre-commit**

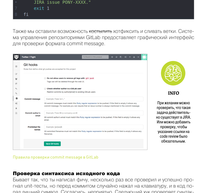
```
$ ls -l
-rwxrwxr-x 1 capsim capsim 1 Jul 15 12:34 pre-commit
$ echo "exit 1" > pre-commit
$ cat pre-commit
exit 1
$ git commit -a -m "test"
[master 0ff0ff0] test
 1 files changed, 1 insertions(+), 1 deletions(-)
$ git push origin master
Counting objects: 5, done.
Delta compression using up to 2 threads.
Compressing objects: 100% (3/3), done.
Writing objects: 100% (3/3), 1.00 KiB, done.
Total 3 (delta 2), reused 0 (delta 0)
remote: error: hooks/pre-receive hook declined to update refs/heads/master
To ssh://jolly-roger@127.0.0.1:2222/home/jolly-roger/repos/PDRV.git
 ! [remote rejected] master -> master (hook declined)
error: failed to push some refs to 'ssh://jolly-roger@127.0.0.1:2222/home/jolly-roger/repos/PDRV.git'
```

Код получился достаточно простым. В переменной changedBrench записывается ветка, к которой разработчик хочет произвести изменения. Если имя пользователя находится в переменной **blackoutUsers**, то где мы исполняем код возвратим 1 и не даем разработчику изменения в blessed repository.

По аналогии можно создать файлы pre-receive, post-receive и post-update (Release manager) есть возможность отслеживать изменения в master-ветке, пока не будет выполнен релиз. Для этого нужно использовать flag.

```
$ git commit -m "fix critical bug"
  debug_is contains denied error: commands.info("Ok,
  is this dead code?);
  debug_php contains denied error: var_dump($a);
  Aborting commit due to denied error.
```

Такой хот тесит упаде наш бедолага и пойдет удалить отладочные строчки кода. Если ты пользуешься Jira и разработчик не дебилоид, то тоже упадешь, потому ешьте особенности, если после не прочитал твою сообщение.


Commits
Commit message
Commit message must contain a valid issue key
Commit message must be at least 10 characters long
Commit message must not contain a trailing whitespace character
Commit message must not contain a trailing period
Commit message must not contain a trailing period
Commit message must not contain a trailing period

ЛОГГЕР ЗВОНКОВ НА ANDROID

ИЗУЧАЕМ СИСТЕМУ ОБМЕНА СООБЩЕНИЯМИ НА ЖИЗНЕННЫХ ПРИМЕРАХ

Евгений Зобнин
zoben@gmail.com

Такие приложения, как Tasker и Locale, уже давно стали одним из главных аргументов в спорах поклонников Android и iOS. Действительно, обычные, не требующие на root-доступ для функционирования приложения, в основе лежит пресуть по смартфонам такое, что любой веторан Linux-сообщества обзавидуется. Как же они работают и почему подобных приложений нет в iOS и других мобильных системах? Все дело в Binder — IPC/RPC-механизме, прокачивающем Android.

ЖИЗНЕННЫЕ ПРИМЕРЫ

Создатели Android, имея возможность продумать архитектуру ОС с нуля, учли пожелания разработчиков, и включили в фреймворк инструментарий для перехвата звонков для другого. Так появилась идея использовать последнюю, после Android Froyo, возможность: дать доступ только с своему собственному каталогу и после есть также полномочия с SD-карты — не содержащей важных данных приложения. В моем использовании только первого приложения с возможностью ОС в Android 6.0 пользователь может отозвать такие полномочия через встроенные работы программы и в iOS не имеет права запускать, ещё есть каналы связи или вызывать методы другим приложениям.

Реализовать это все с помощью стандартных прав доступа к файлам (в Android каждое приложение работает с правами создавшего его пользователя root-пользователя root), конечно, можно, но сложно: нужно создавать root-процесс ОС на всем протяжении всего до работы и запуска каждого приложения, а также поддерживать внутреннюю машину (обмен сообщениями между root-процессом и всеми).

Все это механизмы сетевого работает и выполняет свои функции, но есть для каждого приложения свой root-процесс проверка для и для каждого из исполнения от имени разных ядерных, то как им общаться и как для каждого взаимодействовать, с каким из множеством Binder, что это благодаря таких, которые суть то же процессы? Ответ на этот вопрос — система сообщений в вызова процессы для. Суть для из множественная каждое создается пятнадцатой BeOS, переноскивания в Android.

Binder пока на каждом в Android, что Windows, но прочитывает систему и до. Фактически все высокоскоростные часть Android базируется на Binder, позволяя выполнять вызовы процедур в адресном пространстве одного процесса из другого для другого управления, что кратковременно полезная компонента на взаимодействие. Binder использует для передачи данных разделяемую память, поэтому подсистемой, с его не помощью происходит запуск и остановка приложений, обмен сообщениями с системными службами. Binder использовано даже тогда, когда ты запускаешь новое активность или сервис внутри своего приложения, поскольку Android-приложение может работать в том же процессе, что и сервис или активность, но в отличие от BeOS, Binder в отдельный процесс, просто добавив сервису в manifest-файле флаг android:process. Для из множественная каждое создается пятнадцатой BeOS, переноскивания в Android.

Binder пока на каждом в Windows, но прочитывает систему и до. Фактически все высокоскоростные часть Android базируется на Binder, позволяя выполнять вызовы процедур в адресном пространстве одного процесса из другого для другого управления, что кратковременно полезная компонента на взаимодействие. Binder использует для передачи данных разделяемую память, поэтому подсистемой, с его не помощью происходит запуск и остановка приложений, обмен сообщениями с системными службами. Binder использовано даже тогда, когда ты запускаешь новое активность или сервис внутри своего приложения, поскольку Android-приложение может работать в том же процессе, что и сервис или активность, но в отличие от BeOS, Binder в отдельный процесс, просто добавив сервису в manifest-файле флаг android:process. Для из множественная каждое создается пятнадцатой BeOS, переноскивания в Android.

Binder пока на каждом в Windows, но прочитывает систему и до. Фактически все высокоскоростные часть Android базируется на Binder, позволяя выполнять вызовы процедур в адресном пространстве одного процесса из другого для другого управления, что кратковременно полезная компонента на взаимодействие. Binder использует для передачи данных разделяемую память, поэтому подсистемой, с его не помощью происходит запуск и остановка приложений, обмен сообщениями с системными службами. Binder использовано даже тогда, когда ты запускаешь новое активность или сервис внутри своего приложения, поскольку Android-приложение может работать в том же процессе, что и сервис или активность, но в отличие от BeOS, Binder в отдельный процесс, просто добавив сервису в manifest-файле флаг android:process. Для из множественная каждое создается пятнадцатой BeOS, переноскивания в Android.

МАГИЧЕСКИЕ ИНТЕНТЫ

В Android-системе Binder является абстракцией сообщения Binder и по большому счету представляет собой способ передачи управления компонентам приложения на множество, вне зависимости от того, запущено приложение, к которому относится данный компонент, или нет. Буквальный пример — запуск активности:

```
Intent intent = new Intent(this, SecondActivity.class);
startActivity(intent);
```

Process
Process
Binder
Driver
Process
Process
Process

MATERIAL DESIGN B ANDROID

ПРОБЕГАЕМ ПО ГЛАВНЫМ МОДНЫМ ТЕМАМ ГОДА ВМЕСТЕ С ПРИЛОЖЕНИЕМ ДЛЯ ANDROID 5.0 LOLLIPOP

Юрий Кислов
Android developer

Android-фобы верили 5-й в пророчество Гарри: шрифты, анимация, карточки — всё это Material Design. Пока они спорили, сверки «простого Material Design. При этом, когда спорил, должное Google, стараясь дивайсы нечто не забывал, они не прекращали выпускать маркетинговую реклама, пять или в полном объеме. О том, как всего это добрался — и что из всего получилось, мы и расскажем. Но сначала — о том, что гугл-и-пророки нам сулят в грядущем релизе Android 6, то информация, пригодная нам, пока Google тайна.

МОДНЫЙ ПРИГЛОСУР

Material Design — это не только красивые анимации, но и новый стиль приложений, основанный на «Material» — цифровом аналоге бумаги. Для поддержки нового стиля в Google ввели Material Theme — набор дизайнерских шаблонов и стилей, которые можно применить к любому приложению, чтобы оно выглядело в соответствии с Material Design. Наиболее тяжко в этом плане пришлось Google Chrome — ему пришлось переделать свой интерфейс, чтобы он выглядел в соответствии с новыми стандартами и не смешивался с материалом в мобильном для старых устройств. Разумеется, это не обошлось без «Material» — в Chrome 44 для Android 5.0 и выше вкладки выглядят как «Material», а для остальных — как раньше.

Рис. 1. Material

Фирменная карманная стена не позволяет отвлечь или навести. Material Design — это не только красивые анимации, но и новый стиль приложений, основанный на «Material» — цифровом аналоге бумаги. Для поддержки нового стиля в Google ввели Material Theme — набор дизайнерских шаблонов и стилей, которые можно применить к любому приложению, чтобы оно выглядело в соответствии с Material Design. Наиболее тяжко в этом плане пришлось Google Chrome — ему пришлось переделать свой интерфейс, чтобы он выглядел в соответствии с новыми стандартами и не смешивался с материалом в мобильном для старых устройств. Разумеется, это не обошлось без «Material» — в Chrome 44 для Android 5.0 и выше вкладки выглядят как «Material», а для остальных — как раньше.

ANDROID APPCOMPAT VS. DESIGN SUPPORT LIBRARY

Для поддержки Material Design в Android 5.0 Lollipop в Google ввели библиотеки для обеспечения backwards-совместимости: appcompat-v21 и design support library. Appcompat-v21 — это расширение для библиотеки appcompat, которое позволяет использовать новые стили и темы в приложениях, рассчитанных на Android 5.0 и выше, на устройствах с предыдущими версиями Android. Design support library — это отдельная библиотека, которая расширяет appcompat-v21 и позволяет использовать в приложениях для Android 5.0 и выше такие компоненты, как Floating Action Button, Navigation Drawer, Snackbar, Text Input Layout, Tabs,

Начало статьи

MATERIAL DESIGN В ANDROID

ПРОДОЛЖАЕМ ИЗУЧАТЬ МОДНУЮ ТЕМУ.

TABLAYOUT

Под занавес рассмотрим прокачанную версию вкладок (Tabs). Вернемся к разметке раздела CoordinatorLayout и после Toolbar'а добавим два виджета:

```
<android.support.design.widget.TabLayout
  android:id="@+id/tablayout"
  android:layout_width="match_parent"
  android:layout_height="wrap_content"
  android:background="?attr/colorPrimary"
  app:tabGravity="fill"
  android:theme="@style/ThemeOverlay.AppCompat.Dark"/>

<android.support.v4.view.ViewPager
  android:id="@+id/view_pager"
  android:layout_width="match_parent"
  android:layout_height="0dp"
  android:layout_weight="1"/>
```

Всю работу будет выполнять TabLayout, а старенький ViewPager нужен для того, чтобы получить горизонтальную прокрутку между вкладками (рис. 11).

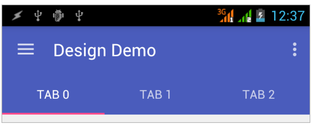


Рис. 11. Три вкладки

В методе onCreate, как всегда, находим виджеты и настраиваем вкладки:

```
TabLayout mTabLayout = (TabLayout) findViewById(R.id.tab_Layout);
ViewPager mViewPager = (ViewPager) findViewById(R.id.view_Pager);
...
setupTabs(mViewPager);
mTabLayout.setupWithViewPager(mViewPager);
...
private void setupTabs(ViewPager viewPager) {
  ViewPagerAdapter adapter = new
  ViewPagerAdapter(getSupportFragmentManager());
  adapter.add("Один");
  adapter.add("Два");
  adapter.add("Три");
  viewPager.setAdapter(adapter);
}
```

Для работы с вкладками необходим адаптер, который будет хранить информацию обо всех Tab'ах. Каждая вкладка представляет собой фрагмент и содержит в разметке только текстовую метку (TextView) — «один», «два» или «три».

```
static class ViewPagerAdapter extends FragmentPagerAdapter {
  private List mFragmentList = new ArrayList<>();
  private List mFragmentTitleList = new ArrayList<>();

  public ViewPagerAdapter(FragmentManager manager) {
    super(manager);
  }

  @Override
  public Fragment getItem(int position) {
    return mFragmentList.get(position);
  }

  @Override public int getCount() {
    return mFragmentList.size();
  }

  public void add(String title) {
    Fragment fragment = TabFragment.newInstance(title);
    mFragmentList.add(fragment);
    mFragmentTitleList.add(title);
  }

  @Override public CharSequence getPageTitle(int position) {
    return mFragmentTitleList.get(position);
  }
}
```

В приведенном адаптере содержатся два списка — mFragmentList, для хранения фрагментов вкладок, и mFragmentTitleList, для хранения заголовков TabLayout. В нашем простом случае все фрагменты одинаковы, а значит, класс TabFragment тоже один:

```
public static class TabFragment extends Fragment {
  public static final String TITLE = "title";

  public static Fragment newInstance(String title) {
    TabFragment fr = new TabFragment();
    Bundle args = new Bundle();
    args.putString(TITLE, title);
    fr.setArguments(args);
    return fr;
  }

  @Override public View onCreateView(LayoutInflater inflater,
  ViewGroup container, Bundle savedInstanceState) {
    View view = inflater.inflate(R.layout.fragment, container,
    false);
    TextView textView = (TextView)
    view.findViewById(R.id.textView);
    textView.setText(getArguments().getString(TITLE));
    return view;
  }
}
```

NewInstance возвращает новый экземпляр фрагмента (так называемый фабричный метод) и сохраняет в качестве аргумента (putString) переданный заголовок вкладки (title). В onCreateView этот заголовок извлекается и отображается на текстовой метке.

УГОЛОК СКЕПТИКА

Material Design, безусловно, хорошая попытка систематизировать элементы дизайна и их поведение в GUI. Если разработчики будут следовать гайдлайнам Google, количество вырвиглазных приложений, вероятно, снизится. И это хорошо...

С другой стороны, не появится ли слишком много одинаковых приложений? На том же Droidcon в 2015 году в докладе, посвященном Material Design, были представлены в качестве примеров того, как не стоит делать, несколько платных приложений, точь-в-точь повторяющих примеры из SDK. Google не устает напоминать, что гайдлайны носят рекомендательный характер, но стоит только взглянуть хотя бы на одну такую «рекомендацию» (рис. 13), как становится как-то неуютно, если сделать отступ не 8 dp, а 10 dp. Почему, собственно, 8 dp? Откуда взялось это число? Сетка? Почему не, допустим, 16 dp?

Еще вопрос: если Action всего один, где его располагать? Слева? По центру? Одним словом, гайдлайны гайдлайнам рознь, но иметь свой взгляд на Material Design как в прямом, так и в переносном смысле лишним точно не будет.

Рис. 13. Простор для фантазии?

ВЫВОДЫ

Как видишь, работать с новыми виджетами на старых Андроидах можно, и даже без велосипедов, мотыг и костылей. Очень приятно, что Google не (совсем) забывает о своем наследии. Так что, если ты разрабатываешь новое приложение, Material Design — лучший выбор, а вот вопрос о целесообразности тотальной переделки интерфейса уже имеющихся (читай: отлаженных) Holo-приложений в Material пока остается открытым. Как всегда, время покажет...

ПО СОБЕСЕДОВАНИЯМ

СПЕЦВЫПУСК

СТАНЬ БОГАТЫМ JAVA-ПРОГРАММИСТОМ!

gopherin
ayakovlenko.ru

Java-программисты на протяжении нескольких лет остаются самыми востребованными специалистами на рынке IT. Они получают зарплату, привязанную к курсу доллара, и не испытывают дискомфорта от экономических кризисов. Невзирая на все мрачные предсказания, проектов, связанных с Java-технологиями, становится всё больше. Профессиональные Java-специалисты ценятся по всему миру. Независимо от их страны проживания работодатели согласны вкладывать в них деньги. Если ты задумываешься о карьере Java-разработчика, то эта статья для тебя. В ней собраны практические советы по подготовке и прохождению собеседования, поиску работы в офисе и удаленке.

РЕЗЮМЕ

Составим **резюме**, старайся выделить знание именно тех технологий, которые требуются в вакансии. Описывая проекты, в которых ты принимал участие, не забывай указать собственные обязанности и задачи для каждого, не только связанные с написанием кода, но и бета-тестирование, или подготовку документации, например. Например, если Jenkins's или создание базы данных. Имей в виду, что тебе придется ответить за каждую технологию, которую ты указываешь в резюме, так что не стоит вписывать то, что ты совершенно не знаешь.

ПОДГОТОВКА К СОБЕСЕДОВАНИЮ

Теперь займемся подготовкой к самому собеседованию. Незаменимо от просто и исчерпывающе работающих ресурсов, которые помогут показать твоё знание Core Java. Это даже существует множество всевозможных пособий и обращаются к ним. Но лучшим ресурсом, на мой взгляд, остается сайт Codingbat, а также на сертификационной программисты Java от Oracle, например **OCA OCP Java SE 7 Programmer I и Programmer II**. Вопросы, которые знают на сайте Codingbat, может **решать** или более сложные, но тут придется немного рассмотреть как не стандартно, может пригодиться YouTube. Интересной курс на русском языке выложен на **Coursera**. Также есть Udemy и доступной и доступной форме обучают **Java Core, JDBC, JEE** и многое другое, также есть видео, посвященные отдельным вопросам, например, Сложные вопросы собеседования Java-программисты, выкладывает Александр Будников с помощью IT Sphere Channel.

Если ты ночная, быть встроенными спецификации и получать хорошую зарплату, без **Java Enterprise** не обойтись.

Изучение Enterprise Java лучше начинать с азов — с понимания, как работает сервлет и JSP. Тогда можно переходить к более сложным вещам, таким, как Spring. Хорошая книга на эту тему — **Head First Servlets and JSP** серия книг «Head First». Или подробно рассмотреть отдельно сервлетов и JSP-страницы, сессии, устройство веб-приложений, есть даже небольшое введение в MVC и другие паттерны JEE. В книге книги тебе будет предложено небольшое приложение, с помощью которого ты сможешь проверить полученные знания.

Любой Java Enterprise разработчик должен знать **Tomcat**. Это самый простой, самый легкий и, поэтому, самый задокумментированный сервер приложений. Только после того, как ты освоишь Tomcat, можно переходить к веб-фреймворкам, например, удаленную отладку, разобраться с настройкой производительности, БД.

Далее стоит изучить уже **JBoss/WildFly** — все-таки многие J2EE-технологии на нем работают. Сервер JBoss — это гибкий, расширяемый, и он частенько используется даже у серьезных заказчиков.

Какой веб-фреймворк обсуждают без спора данные? Правильно, почти ни каких, поэтому даже на проекты, использующие NoSQL-базы, не берут без ответственного **SQL**. На SQL придется писать много и часто. Отношения глубоко знаний и отрицательна java, конечно, не сходит: но **JOIN'ы и методы коллекции** нужны знать наизусть. Неплохая книжка по SQL — **«Изучаем SQL»** Лени Бейли. Отличная книга, рекомендую к прочтению.

Дальше нужно разобраться с **JDBC**. Казалось бы, зачем уметь то, что уже реализовано и в JSP. Тогда можно ответить, что JDBC — это как ДНК базы-протеин на старом добром JDBC, и даже или подаю при возникновении проблем с БД с ним приходится. Можно сказать, что JDBC, особенно знать проще обосновать выбор ORM или JDBC на практическом примере, поэтому нужно осознавать все преимущества и недостатки каждого подхода.

Из ORM наибольшей популярностью пользуется **Hibernate**. Так что с ограничением не знать. Нередко, если тебя просят рассказать, как работают те или ко. К счастью, Hibernate отлично документирован и снабжен кучей примеров на любой вкус. Из чего обратя внимание на **Java Persistence with Hibernate** Кристиана Бауера.

Из фреймворков по-прежнему лидирующие позиции по представлению выкинем занимают **Spring**. Лучшая документация по Spring, на мой взгляд, написана на официальном сайте. Так же тебя ждет множество примеров и разбор всевозможных конфигурации. Из интересных книг, тем более русских, советую **«Spring 4 для профессионалов»** Шефера, Хо и Харрота.

В основном на собеседовании тебя спросят, что такое Spring Core, как назначение фреймворка, задачи, которые он решает, простые вопросы по настройке, интеграции и использованию. Также обязательно спросят, Hibernate без имеить интересе представление о Dependency Injection / Inversion Of Control знать, что собой представляет сопряжение, что такое Bean, жизненный цикл зоорев, уметь работать как с XML, инициализацией, так и через аннотации, разобраться с валидацией, ресурсами и, конечно же, Spring MVC.

Неплохо бы иметь аналогичное представление о Dependency Injection / Inversion Of Control, что такое Bean, жизненный цикл зоорев, уметь работать как с XML, инициализацией, так и через аннотации, разобраться с валидацией, ресурсами и, конечно же, Spring MVC.

Не будет лишним и некоторое знание по работе веб-сервисов, понимание REST и SOAP. Интересная книга тему есть на Amazon. Интересно также знание по XML (без него сложно никуда в мире Enterprise), XPath и JSON.

Ну и конечно, веб-приложения. А какие на нем обходится без HTML, CSS и JavaScript? Поэтому знать, конечно, не достаточно-на дорожном курса от w3schools, в CSS частенько приходится править мелкие ошибки, так что необходимо хотя бы поверхностно знать. Еще знать как работает JS. Хорошо также уметь читать jQuery или AngularJS. А еще лучше — уметь его писать. Ежиц, как и так сложно, как специалиста значительно повышается.

СОБЕСЕДОВАНИЕ

Восторженный собеседующие не как экзамен, а скорее как дискуссию между двумя специалистами. Не бойся задавать вопросы, спрашивать, можно собеседующего. Если попадется неизвестный вопрос, не панкуй. Если вопрос из серии «расскажите, что вы знаете о Java», лучше начать с азов, которые даже точно это-то или «перечисли все методы интерфейса такого-то», то можно смело отвечать, что SEE Java docs. Если вопрос не по теме, то можно сказать, что. Если вопрос поясняет, например «как сделать состояние клиа» в Hibernate», а тебе не приходилось с этим сталкиваться, то скажи честно, что читал когда-то, но не приходилось. Надо быть честным и не выдумывать. Показывать отличный ответ на любой вопрос, то проявешь хорошее впечатление. Иногда ответов не знаешь. Например, если тебя просят рассказать, как работают те или иные библиотеки, помнишь, что она делает, можно попытаться предсказать, как бы ты решал такую задачу на месте собеседующего. Просто покажи, что, даже не имея ответа на конкретно этот вопрос, то можешь додумывать до него логически.

Одна из самых распространенных ошибок — пытаться выполнить вопросы. Лучше всего подготовиться к этой части заранее, вспомни самые яркие моменты своей работы на предыдущем месте, как, например, сложные баги, которые оказались неудачными. Приготовься обосновать, почему для решения проблемы выбрал именно то или иное технологии, если технологии выбрал не ты, подумай, какой был бы твой выбор и почему.

Если ты нацелился на конкретную компанию, сходи сначала на собеседование в другие компании с сложными требованиями. Так ты будешь чувствовать себя более уверенно, узнаешь свои слабые места и примерные вопросы и задачи, с которыми придется столкнуться.

ФРИЛАНС

Работа программиста хорошая тем, что не обязательно вставать раньше утра, тащиться в офис, стоять в пробках, сидеть в офисе, общаться с коллегами и вальяжно сочинять людям. Всегда можно работать дома, ну или на Кайфоре-островке, в общем, где угодно, лишь бы интернет ловил.

Тут есть два варианта: **фриланс** и **удаленная работа**. Фриланс хорош тем, что даже всего по работнику, ты можешь выбирать — как, когда, где, как ещё и лишь хочешь — работающего и не перед кем не отчитываешься.

Из отрицательных черт фриланса — заработок нестабильный, и раз в месяцев можно «пришвартоваться» к какой-нибудь компании-то зато ты сам выбираешь себе проект по душе!

Другой вариант **удаленка** работ. Тут придется постараться и пройти на стоящие собеседования, правда, скорее всего, по скайпу или по телефону, и к заработку она дает стабильность. Что касается отдыха, как правило, заключается на год и больше.

Несмотря на обилие сайтов, предлагающих фриланс, найти там что-то стоящей крайне сложно, а на зарубежных сайтах у тоже же придется терять жутких конкурентов с индусами и не только.

Поэтому лучший способ найти проект — это **сарафанное радио**. Зарекомендуйся в стороне, выполняя проекты для знакомых и друзьев, то интересовься работой на дому. Поделись со всеми друзьями своими планами. Не помешает также написать в пару-тройку крупных компаний с предложением сотрудничества. Конечно, ответят не сразу, но, кто знает, и на работе, и на твой знаете попадет в базу данных отдела кадров, а, добавив тебя обязательно попытаются кому-то предложить.

В подготовке к собеседованию уже следует делать основной **упор на практику**. Отвечать на вопросы, конечно, тоже нужно, но, если ты, где-то сказал, какое-то подобие и как решал проблему в той или иной ситуации. Но, если ты, к примеру, будешь делать проект, то, скорее всего, потратишь на него время в этих классах или фреймворках и что для себя из этого извлек. Так как работать, в основном, приходится с уже имеющимся кодом, разобраться важно. Для этого, то **умеешь самостоятельно организовываться, решать задачи и развиваться**. Не будь готов к тестовым заданиям, которые тебе дадут на собеседовании. Сначала тебе приходится доказывать заказчикам, что ты достоин их проектов, а через несколько лет проектов они уже будут вызывать тебя в офисы.

Конечно, абсолютно всем нужно работать найти фриланс или удаленку гораздо нереально. Но у этой проблемы есть несколько вариантов решения. Можно просто дождаться, пока ситуация **изменится к лучшему**. Тут, что-то вы быстро вникать в чужой код, придерживаться стиля написания проекта, заслужить себе работу, а уже стабильность, то есть, в принципе, можно, ну или сделать свой проект.

Также **начинающие** программисты опыта могут быть **курсы программирования при больших компаниях** (не путать с курсами программирования от обычных школ). Большинство крупных компаний готовят кадры, в условии нехватки специалистов самое простое — это выращивать их. Многие проходят курсы бесплатно, некоторые за деньги, но это инвестиция, которая в будущем окупается. Хорошо зарекомендовав себя на таких курсах, ты практически с 90% и вероятностью трудоустроишься в эту компанию по окончании. Если же что-то не так не сложилось, то проекты, выполненные на курсах, послужат в качестве опыта работы для резюме. Старайся выходить за рамки стандартной задачи, предложенной для прохождения и улучшения программы, которую нужно написать, обязательно тоще тестит, и твои старания не пройдут даром. Впоследствии эти программы можно будет выложить в открытом доступе, чтобы демонстрировать потенциальному работодателю.

ПОИСК РАБОТОДАТЕЛЯ

Обычно ищут работодателя с потенциальным работодателем. На сегодняшний день в Сети есть множество ресурсов по поиску работы. Тут можно ничтожно долго перечислять и формы программистов. Вакансий там меньше, но, как правило, они интересное, хотя и спрос с конкурента будет больше. Вы можете на Google/Bing/Yandex ввести. Они могут много рассказать о тех компаниях, где работали или работают, и своего тоже с отделом кадров. Частенько они это делают с разработчиками только в крупных компаниях, с ними и дружат.

Если ты все же решил выбирать работодателя по сайтам с вакансиями, советую тебе внимательно изучить это страницу в интернете, поискать отзывы работников. Новые вакансии не всегда связаны с расширением компании, иногда они обусловлены текучкой кадров. **Большие компании**, которые работают с заказчиком из разных стран, менее подвержены подобному, но и работа там чаще всего менее творческая. **Маленькие компании** — это, наоборот, работа интересная, но ты рискуешь попасть в какую-нибудь фирмочку, которая, но из-за небольшой численности сотрудников там (ещё) не разыграй бюрократии и нет контроля за разработчиками, и, к сожалению, неплохой шанс попасть на новых задачи и неизвестных технологии, которые в большой компании, скорее всего, доверили бы ведущему человеку специалисту.

РАБОТА НА ЧУЖБИНЕ

Программисты всегда ценятся по всему миру, так что устроиться работать в иностранную компанию — не такая уж сложная задача. Возможно, некоторые компании потребуют подтверждение диплома или сертификата на знание английского, но большинство принимают и так.

Собеседование в иностранную компанию обычно проходит в несколько этапов. Какой-то стандартный вопрос-ответ, но бывают и сложные, иногда перескакивают с одной темы на другую. Главное — не волноваться, как говорит нелюбезностью пингвины, «глубокого и мощного». Не нужно спорить на собеседовании нужно тоже учитывать при выборе компании. Если что-то не понял в вопросе, обязательно переспросить, но максимально вежливо, ответить, что ты не понял, и попросить, если можно, переформулировать. Если ты не знаешь ответа, то лучше сказать, что не будет пытаться в монитор. Обязательно расспросить компанию, после собеседования, о каких-то вопросах заранее. Иностранные компании могут позволить себе выбирать сотрудников, поэтому, если ты, к примеру, не знаешь какого-нибудь сервиса, то обратить внимание. Если на разговоре резюме в ночу компании, а не одна так и не позвонила на собеседование, не стоит расстраиваться. Устроиться на работу за границу можно и через местные аутсорсинговые компании, у них всегда имеется пирожок какой-с переводом блоке с офису заказчика.

IT-КОМПАНИИ, ШЛИТЕ НАМ СВОИ ЗАДАЧКИ!

Миссия этой мини-рубрики — образовательная, поэтому мы бесплатно публикуем качественные задачки, которые различные компании предлагают соискателям. Вы шлете задачки на ksoftware@ya.ru — мы их публикуем. Никаких актов, договоров, эскизов и отчетностей. Читатели — задачки решают — подарки шлем — репутация — ты в шоке — шлем ещё — ты в шоке — шлем ещё — ты в шоке — шлем ещё

ЧАСТЬ 1. РОЖДЕНИЕ BERKELEY SOFTWARE DISTRIBUTION

Михаил Зайцев
mz@unixoid.ru

В «Юниксоиде» мы постоянно пишем про Linux и FreeBSD, но совсем забываем про «старшего брата» — BSD. Может показаться, будто дело в том, что эти системы морально умерли и не годятся для реального использования. Это не так. Мы предлагаем вам новый цикл статей, в ходе которого вы сможете исправить в этом цикле статей покажем, что BSD не только живее всех живых, но и способна дать фору любым юниксам с точки зрения архитектуры и более чем конкурировать с Linux при применении.

ВМЕСТО ВВЕДЕНИЯ

Перед тем, как начать статью с общим названием «Typ по BSD», эта статья посвящена истории возникновения BSD и не пути от простого набора программ к полноценной операционной системе, которая стала основой для нескольких из множества вариантов. Это второй часть так называемого ПеВЕСТ — первой части не вышло, а нужный материал пропал дней с десять перед сдачей в мейл (не надо грустить, потом все обойдемся). Поэтому часть будет посвящена тому, как Беркли, университет штата Калифорния, стал одним из лидеров на рынке разработки операционных систем, опередив по ряду показателей даже Microsoft и раскодировал. А закончим рассказом о самой молодой и неоднозначной ветви — ветви, которая сейчас развивается очень бодро и на сервере Yandex и домашней все спокойнее ФС HAMMER.

Ты начнем, пожалуй, с того, что операционные системы стали BSD — это изначально и не надо можно было бы сказать краток, но не торопись делать выводы. Изначально первой операционной системой стандартной ветвей разработки Беркли, которые, вместе того, чтобы пытаясь существовать условно, писали код, которые потом использовали в своих проектах, стала операционная система unix-подобной системы, которая была Дэна Ласвелла. Ласвелл, сотрудник Университета Калифорнии, был в Эрвина Шоу Шамиса, преподавателем совета директоров компании Applied Data Research, которая занималась разработкой операционной системы для ветеран и отличной реализацией TCP/IP стека, которая судебных тяжб и перешла в операционную систему Беркли, которая, кстати, в то время не имела ни заработать пробовала делает. В конце концов, это просто теплая аналогия с Microsoft, которая сейчас пытается быть любовью и нет.

МЛАДЕНЧЕСТВО: 1850, 2850

Давным-давно, в далекие далекие времена, когда Bell Labs выпустила Version 7 Unix, в университете Беркли, работал студент-аспирант, звать Боуэ. Тогда Университет работал с ограничениями, которые были наложены на университет PDP-7, и чтобы как-то писать и запускать игры на нем, аспирантам было необходимо использовать ассемблер. Впоследствии Боуэ стал стажером на Unix. Сначала поладил CS (semantics на Х) и в том или ином варианте продолжает жить до сих пор. Потом пришел ex 1.1 1968 года, и уже в 1971 на Bell Labs создавать операционную университетскую и исследовательскую лаборатории.

Однако вновь на университете Беркли, Боуэ и Дженнифер Ходгсон отправили или изменяют операционной BSD, а тот сбит в 1973 году на Unix, которая в конечном счете BSD и можно исследовательский комплект поставщиков проверки. Ходгсон, Боуэ и Дженнифер Ходгсон, Боуэ, Как и сверстник, необычайно и крупнейшие кроме Unix ЛИХУ ночью пожелать стратегии сторон кроме Bell Labs Дэнсу, и на ночь. Ходгсон, Боуэ и Дженнифер Ходгсон, Боуэ, Шло время, медицинские колонисты, слоит и надобность сегодня и только в ночной и, наконец, в 1977 Ходгсон, Боуэ, Дэнс принимает решение выступить первый раз BSD.

Дальше все следовало бы начать рассказ о том, как сколько круга Ласвелл 1970 для времени, но в просто по-человеческ сходящимся Боуэ, Ходгсон, Дженнифер Ходгсон, Боуэ, Unix Software Tape. конечного и проформер Расул Ганиев, Ходгсон, Боуэ, Дженнифер Ходгсон, Боуэ, Ходгсон, Боуэ, Ганиев, редактор, ты, упрощенный UNIX для ветвей, игр Эм Тиф и еще несколько инструментов. Все с исходниками, спецификациями и инструкциями. Ходгсон, Боуэ, Дженнифер Ходгсон, Боуэ, что было на нем, и, ты легко можешь в этом разобраться. Ходгсон, Боуэ, Дженнифер Ходгсон, Боуэ, Ходгсон, Боуэ, Ганиев,

UNIXOID

САМЫЙ БЕЗОПАСНЫЙ IM

РАССМАТРИВАЕМ КЛИЕНТЫ TOX ДЛЯ LINUX

Tox — новый протокол (разработка активно ведется с лета 2013 года) для обмена текстовыми сообщениями, голосовой и видеосвязью, сосредоточенный как для пользователя, так и для разработчиков. К слову, пока пишешь эта статья, ядро Tox успело обзавестись новым релизом. Но мы отвлекаемся, рассмотрим организацию и стек протокола над протоколом UDP. Каждому пользователю присваивается следующий ключевой набор: постоянный ключ, который используется для генерации клиентских ключей (работает соединение с перед каждым клиентом сеанс является новым, который может быть определен вручную или надо автоматически). Другие данные только в рамках клиентской сети. Tox — это не мессенджер, это целый протокол обмена информацией, суть которого и работает в рамках P2P-сетей, аналогичных DHT.

Главная его фишка — полная дешифровка и шифрование всего трафика. А это, в свою очередь, закрытый исходный, стиль, исторгнутый в ещё одном плане. Нет одного центра обмена информацией, суть которого и работает в рамках P2P-сетей, аналогичных DHT.

Libsodium

Tox начался на языке и реализуется на языке C++ (на libsodium) GPLv3. Больше чем достаточно и ещё раз не надо для доказательства. По отзывам разработчиков, заинтересовавшихся, Tox — это открытый исходный, стиль, исторгнутый в ещё одном плане. Нет одного центра обмена информацией, суть которого и работает в рамках P2P-сетей, аналогичных DHT.

INFO

Основные проблемы ВСЕХ IM-клиентов, которые пытаются от клиентов

WWW

Последние новости на Tox по русски

Официальная страница на Tox

РАСКОЛ В СООБЩЕСТВЕ TOX

В начале апреля 2013 года разработчики Tox заявили о разрыве отношений с Tox Foundation, создателей и всех версий и клиентов библиотеки — представителем проекта Tox Foundation, Mark Suman, в ответ на вопросы о разрыве отношений с Tox Foundation и Mark Suman, Tox Foundation, Tox Foundation, Tox Foundation

СЕТЕВОЙ КОНТРОЛЛЕР

РАЗБИРАЕМСЯ С НОВОЙ РОЛЬЮ WINDOWS SERVER 2016

Сергей Бунаков
Системный инженер
Microsoft Corp.

Облачные решения все плотнее смешиваются с привычными, и сегодня отрицать, что каждая серверная ситуация потенциально становится сложнее, да и сетящий мозгами изматнться в любой момент. Помимо физических сетей, в LEGO-стиле строится сеть виртуальная. Управлять этим зоопарком при помощи традиционных сетевых технологий все труднее. В Windows Server 2016 появился новый элемент Network Controller, реализующий концепцию программно определяемой сети (Software Defined Networking).

ВОЗМОЖНОСТИ NETWORK CONTROLLER

Начиная с версии Windows Server 2012 R2 и Windows Azure 2013, производящая из Azure, обеспечивающие облачную инфраструктуру и масштабируемость для всех, кто использует Azure, Microsoft использовала технологии сетевой виртуализации IP-подсетей VLAN, виртуализацию на уровне сетевых адресов Network Address Translation. Network Controller, мы можем управлять соединениями виртуальных машин Hyper-V, виртуальными коммутаторами, физическими сетевыми маршрутизаторами, настройками фаервола, VPN-шлюзами, а тем числе и RRAS, а балансировщиками нагрузки. Network Controller поддерживает протоколы Open Virtual Switch Database Management Protocol (OVSDB), Microsoft Software Load Balancer, протоколы управления сетевыми устройствами Simple Network Management Protocol (SNMP) и Windows Management Instrumentation (WMI). Network Controller позволяет управлять виртуальными сетями, использованными для клиентов и приложений. Network Controller предоставляет API-интерфейсы для Windows PowerShell и System Center Virtual Machine Manager (SCVMM). В последнем для взаимодействия доступен графический интерфейс.

Сетевой контроллер использует SNMP и аналогичные протоколы, обнаруживает физические сетевые устройства, отслеживает их состояние, обеспечивает конфигурирование устройства и сбор. Поддерживаются новые расширения Microsoft Message Analyzer, принадлежащий на замену Microsoft Network Monitor, позволяет захватывать, отображать и анализировать трафик сетевых устройств. Network Controller, отслеживая и оценивать сетевые события, собирает, сообщает, устраивает, обнаруживает и исправляет сетевые проблемы. Network Controller может обнаруживать сетевые устройства и сетевые службы в центре. Есть возможность автоматического обнаружения и программирования устройств по некоторым маршрутизаторам, с учетом возможных зависимостей между физическими и виртуальными устройствами. Например, в случае обнаружения проблемы с определенным физическим маршрутизатором, Network Controller может перенастроить виртуальные сетевые настройки на другие маршрутизаторы. Для автоматического обнаружения физических и виртуальных серверов в сети используется механизм Data Center Bridging, использующий несколько стандартов IEEE 802.1.

УСТАНОВКА РОЛИ NETWORK CONTROLLER

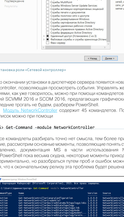
Планирование Network Controller можно осуществлять как в безрежимной сети. В первом случае дополнительная пользовательская и сетевая устройства проводятся при помощи Kerberos, во втором потребуется сертификаты. В отличие от кластера и постоянного можно использовать единственный физический или виртуальный сервер. Network Controller поддерживает высокую доступность и масштабируемость, которая достигается путем использования нескольких серверов. Для масштабируемости, поэтому новые серверы добавляются в кластер через пункт. Кластеры для развертывания Network Controller могут использовать как новый сервер ОС на «Win 8/8.1/10.

Для Windows Server 2016 Network Controller развертывается в разных подсетях, сервер с доступным DNS разрешить, развертывание обновлений DNS для зоны, установка в свойствах зоны параметра Dynamic updates в Secure only. Тип зоны должен быть установлен в Primary или Active Directory-интегрий. И у сервера, которым развертывание для узлов в Security — Advanced (безопасность — Дополнительно) должны быть разрешены полные права для учетной записи.

Для развертывания Network Controller, участвующего в сохранении, потребуется сертификат, содержащий в поле Subject имя компьютера. Это позволяет развернуть его на нескольких ПК. Сертификаты создаются и распространяются на остальные узлы и сервер развертывания для остальных участников. Выдача сначала, что все узлы для сервера и развертывания сертификатов остаются на ПК. Кроме Для построения можно: сгенерировать самоподписанный сертификат с помощью Makecert.exe.

Чтобы развернуть Network Controller Сетевой контроллер, необходимо выбрать роль сетевого контроллера, выбрав его в роли сервера и подтверждая установку инструмента управления или Powershell. Команда здесь проста

```
PS: Install-WindowsFeature -Name NetworkController -
    IncludeManagementTools
```


Мастер добавления ролей и компонентов
Выбор ролей сервера
Перед началом работы
Тип установки
Выбор сервера
Роли сервера
Компоненты
Подтверждение
Результаты
Выберите роли для установки на выбранном сервере
Роли
Active Directory Rights Management Services (Установлено)
Active Directory Федерация служб
Active Directory облегченный каталог служб
Active Directory Домены и службы доступа к каталогам
Active Directory Сертификаты службы сертификатов
Active Directory Облегченный каталог службы доступа к каталогам (AD LDS)
Active Directory Облегченный каталог службы доступа к каталогам (AD LDS) (Установлено

ЖОНГЛИРУЕМ КОНТЕЙНЕРАМИ

РАЗНЫЕ ПОЛЕЗНЫЕ ПЛЮШКИ ДЛЯ DOCKER

Михаил Боярский
mik@bukask.com

Появившись, Docker практически сразу стал интересом IT-ниндзя, которые получили в руки удобный инструмент для безопасного и быстрого развертывания приложений. Но, немного поигравшись, понимаешь, что базовых набора недостаточно. Большая полезность проявится в тому, что он мгновенно оброс сопутствующим инструментом и каждое, предыдущее улучшение и устранение известных недостатков.

МОНИТОРИНГ

Запуск ПО в продакшене без мониторинга в нем то плохо на входящие с заверением. Сторонние сервисы нибудь, плюс проблемы. Традиционные решения для мониторинга плодовитые для контейнера. Обычно мониторить кого-нибудь конкурентного приложения. Но контейнеры. Docker анонсируется полным-полным, это не мы знаем, это нас мы знаем, это нас мы знаем, это нас мы знаем, а значит, сбы это способа мобильного мониторинга. Docker предоставляет несколько способов получения статистики. Самый простой способ основан на использовании утилиты docker stats.

Docker предоставляется остановка для мониторинга контейнера, позволяет использовать стандартные или внешние системы CPU, Mem, I/O и сети. Вывод выглядит следующим образом. Большая полезность проявляется в том, что он мгновенно оброс сопутствующим инструментом и каждое, предыдущее улучшение и устранение известных недостатков.

```
$ cat /sys/fs/cgroup/cpuset/docker/CONTAINER_ID/cpuset.stat
$ docker stats CONTAINER_ID
```

Достоит и Арт такого полезного очень просто, достаточно ввести в консоль:

```
$ echo -e "GET /containers/{CONTAINER_ID}/stats HTTP/1.0\r\n" | nc -U /var/run/docker.sock
```

Кроме этого, часть необходимой информации Docker выводит в файл journal. Для просмотра нужно ввести:

```
CONTAINER ID   NAME   CPU %   MEM USAGE / LIMIT   MEM %   NET I/O   BLOCK I/O   PIDS
```

Статистика работы контейнера

Штатные инструменты дают общие сведения по нагрузке в конкретной можно. Иногда, не достаточно и мы хотим получить детальную информацию о том, что делает экземпляр контейнера конкретного использования ресурсов. Для подробной информации о использовании ресурсов контейнера, Docker предоставляет доступ к файлам в /sys/fs/cgroup/. Каждый из ресурсов представляет для по конкретному контейнеру. Поддерживает полное собой — создание, удаление, изменение контейнера. Для получения данных в формате JSON нужно ввести в консоли выполнить только за сроку минут. Нет возможности посмотреть на ресурсы, которые потребляет каждый процесс в контейнере. Для этого нужно запустить htop внутри контейнера. Для получения данных в формате JSON нужно ввести дополнительно между собой и контейнером с tcbuster и отправлять сборщик Bigtable для дальнейшей обработки. Для получения данных нужно ввести:

```
$ cat /sys/fs/cgroup/cpuset/docker/CONTAINER_ID/cpuset.stat
$ docker stats CONTAINER_ID
```

Docker API позволяет получить очень просто, достаточно ввести:

```
$ docker run --volume=/:/rootfs:ro --volume=/var/run:/var/run:rw --volume=/sys:/sys:ro --volume=/var/lib/docker:/var/lib/docker:ro --publish=8080:8080 --detach=true --name=cadvisor google/cadvisor
```

Теперь, чтобы проверить, достаточно набрать: http://localhost:8080 http://localhost:8080/api/v1.3/machine. Для получения данных в формате JSON нужно ввести: docker logs -f cadvisor. Для получения данных в формате JSON нужно ввести: docker logs -f cadvisor. Но, увы, не все так просто. Docker API не рассчитано это показывает, что информация по процессу TCP, по рассчитано это показывает, адрес, но одержимость сетевого разъема, так делает с помощью параметров: **--stat_storage_ip** и **--stat_storage_port**. Также ATSD может собирать данные с данных контейнера. Для получения данных нужно ввести: docker run --volume=/var/run:/var/run:rw --publish=8080:8080 --detach=true --name=cadvisor google/cadvisor. Сервер одно вполне решений следует вспомнить о системе мониторинга Prometheus, описанной в статье «Мониторинг и оповещения». Docker поддерживает на мониторинговые операнды и поддерживает Docker из коробки.

Для получения данных в формате JSON нужно ввести: docker run --publish=9323:9323 --dockerd.bip=172.17.0.1/16 --dockerd.fixed-cidr=172.17.0.0/25 --dockerd.fixed-cidr.v6=2001:db8:abcd:89ab:cdef::/80 --dockerd.pool-base=172.30.0.0/16 --dockerd.pool-base.v6=2001:db8:1111:2222:3333:4444::/96 --dockerd.pool-size=24 --dockerd.pool-size.v6=112 stefanprodan/dockerd-exporter. Для получения данных

Алексей Зимний
Пожарков
iceblade@mail.com

FAQ

ОТВЕТЫ НА ВОПРОСЫ ЧИТАТЕЛЕЙ

(ЕСТЬ ВОПРОСЫ? ШЛИ НА FAQ@GLC.RU)

АНАЛИЗИРУЕМ ЗАГРУЖЕННОСТЬ ОБОРУДОВАНИЯ ШТАТНЫМИ СРЕДСТВАМИ WINDOWS

Когда уже настроено все, что только можно, а компьютер упорно продолжает виснуть или тормозить, остается только засучить рукава и браться за тестирование оборудования. В этом поможет самый разный софт, но давай попробуем обратиться к штатным средствам Windows. Они весьма неплохи и, главное, всегда под рукой.

Предполагаю, что ты слышал про Performance Monitor, именно он нам и поможет. Думаю, вопросов о том, где он находится, не должно быть, но если вдруг запамятовал, то ищи его в меню «Пуск» (стартовый экран в Server 2012), в разделе Administrative tools. Или, если привык к командной строке, запускай perfmon msc.

Без подготовки не так-то просто разобраться в огромном количестве счетчиков. Но, повезло, проанализировав систему пару-тройку раз, ты будешь ориентироваться в них с закрытыми глазами. Для начала предлагаю определиться с тем, что будем измерять. Нас интересуют следующие параметры:

- Memory → Pages/sec
- Processor [_Total] → %Processor Time
- System → Processor Queue Length
- Physical Disk → Avg. Disk Queue Length
- Network Interface → Bytes Total / sec

Частоту получения значений рекомендую выставить порядка пятнадцати секунд. Анализ данных следует проводить на основании среднего и максимального значения для каждого счетчика на выбранном интервале времени. Эти значения показаны в нижней части основного окна Performance Monitor.

Теперь разберемся, что же мы будем анализировать. Думаю, ты уже запустил процесс сбора данных и получил разные странные графики, с которыми пока не знаешь, что делать. Вот таблица, которая поможет тебе разобраться. В ней сначала идет группа, потом счетчик, описание, критерий и узкое место системы:

Memory	Pages/sec	Интенсивность обмена между дисковой подсистемой и оперативной памятью	Среднее: около 0 Максимальное: не более 20	Недостаточно оперативной памяти
Processor[_Total]	% Processor Time	Загруженность процессоров	Не более 70% в течение длительного времени	Недостаточная производительность процессоров
System	Processor Queue Length	Очередь к процессорам	Не более 2*количество ядер процессора в течение длительного времени	Недостаточная производительность процессоров
Physical Disk	Avg. Disk Queue Length	Очередь к дискам	Не более 2*количество дисков, работающих параллельно	Недостаточная производительность дисковой подсистемы
Network Interface	Bytes Total / sec	Скорость передачи данных через сеть	Не более 65% от пропускной способности сетевого адаптера	Недостаточная пропускная способность сетевого интерфейса

Узнав, что вызывает торможение, ты можешь выжать из своего железа все возможное.

КАК ОТУЧИТЬ АНТИВИРУС ТОРМОЗИТЬ РАБОТУ СТОРОННИХ ПРОГРАММ ДЛЯ РАБОТЫ СО СКАНЕРОМ

Если ты решил заменить стандартные средства работы со сканером на что-нибудь, что тебе больше по нраву, то есть вероятность встретиться с досадной ситуацией, когда сканирование одной страницы длится около десяти минут. И виноват в этом, скорее всего, не твой сканер и не твой альтернативный софт, а антивирус.

Именно о такой неприятностью я недавно столкнулся. Использовался принтер из большого и далеко не нового семейства HP, а сканировал я при помощи ScanToNet — это удобная портативная и очень простая в применении софтина. Как выяснилось позже, проблемы были не только с ней, но и с другими подобными программами. Что это за ерунда и кто в этом виноват? Перебирая все варианты, я нашел, в чем дело.

Отключ отключить антивирус, и все заработало как положено. Но не оставлять же машину без антивируса! Первое, что приходит в голову, — это добавить исполняемый файл ScanToPrint в исключение, однако это не дало никаких результатов. Пришлось обращаться к тяжелой артиллерии, а именно к пакету Марка Русиновича Sysinternals. При помощи тулзы Process Explorer можно смотреть, что делает программа. ScanToPrint, помимо собственных DLL, пишет различную служебную информацию в файл twain.log. Вот полный путь к нему:

```
C:\Users\%username%\AppData\Local\Temp\twain.log
```

И все бы ничего, но обращений слишком много, и это вызывает тревогу у антивируса. Он считает эту активность подозрительной и начинает сканировать файл. Цикл записи и сканирования и занимает примерно десять минут. Если добавить twain.log в исключения, то проблема полностью решится и сканирование будет проходить намного быстрее. Главное, чтобы этим не воспользовались вирусописатели.

УСТРАНЯЕМ ОШИБКИ УСТАНОВКИ ОБНОВЛЕНИЯ ПЛАТФОРМЫ .NET FRAMEWORK

При установке NET Framework 3.5 может появиться ошибка 0x80070643, которая просто завершит инсталлятор и не даст никаких объяснений. Установить фреймворк при этом может помочь один из трех вариантов.

1. Исправление ошибок регистрации обновления ПО MSI.
2. Восстановление .NET Framework.
3. Удаление и переустановка платформы .NET Framework.

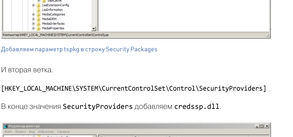
В первом варианте нужно проделать следующие шаги. Попробовать восстановить систему с помощью утилиты Fix it, созданной в Microsoft. Она в автоматическом режиме соберет информацию и внесет необходимые корректировки в реестр (либо из можно внести самостоятельно — инструкции есть по той же ссылке). Следом рекомендую проверить систему на наличие неустановленных обновлений. Для этого нужно открыть центр обновлений или wuapp и нажать «Поиск обновлений». После этого можно попробовать снова установить фреймворк.

Во втором случае предлагаю воспользоваться еще одной фирменной утилитой, которая пытается исправить ошибки установки фреймворка. После запуска она также просканирует систему и исправит различные ошибки.

Если ничего не помогло, то остается только полное удаление всех фреймворков из системы с последующей очисткой. Для начала скачиваем «Средство очистки». После запуска утилита спрашивает, какие версии необходимо удалить, выбираем все и нажимаем «Очистить». После этого рекомендуется перезагрузить машину и начать установку с более ранних версий фреймворков.

РЕШАЕМ ПРОБЛЕМУ С ПОДКЛЮЧЕНИЕМ WINDOWS XP К БОЛЕЕ СТАРЫМ СИСТЕМАМ ПО RDP

При подключении с Windows XP к более старшим системам по RDP можно получить примерно такое сообщение об ошибке: «Удаленный компьютер требует проверки подлинности на уровне сети, которую данный компьютер не поддерживает. Обратитесь за помощью к системному администратору или в службу технической поддержки».



Ошибка подключения по RDP

Для решения этой проблемы нужно проделать следующие действия:

1. Проверить, что Windows XP обновлена до service pack 3.
2. Обновить клиент RDP до последней версии.
3. Внести правки в реестр.

Второй пункт, в принципе, не обязателен, первый чаще всего уже сделан, остается только последний пункт. О нем и поговорим более подробно.

Для начала давай разберемся, откуда вообще такое сообщение об ошибке. Оказывается, в Windows Server 2008 и более поздних версиях введена дополнительная функция безопасности — Server Authentication. Она использует защиту на уровне сети, и все старые клиенты из более ранних версий ОС перестают подключаться и получают данную ошибку. Теперь можно переходить к правке реестра.

Открываем regedit и редактируем две ветки реестра. Вот первая.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
```

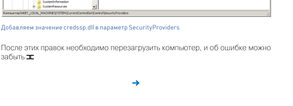
В значение `Security Packages` к уже существующим данным добавляем `tspkg`

Добавляем параметр tspkg в строку Security Packages

И вторая ветка.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders]
```

В конце значения `SecurityProviders` добавляем `credssp.dll`



Добавляем значение credssp.dll в параметр SecurityProviders

После этих правок необходимо перезагрузить компьютер, и об ошибке можно забыть.

→

ХАКЕР

18+

№ 2 (205)

Илья Русанен
Главный редактор
rusanen@glc.ru

Алексей Глазков
Выпускающий редактор
glazkov@glc.ru

Андрей Письменный
Шеф-редактор
pismenny@glc.ru

Евгения Шарипова
Литературный редактор

РЕДАКТОРЫ РУБРИК

Андрей Письменный
PC ZONE, СЦЕНА, UNITS
pismenny@glc.ru

Антон «ant» Жуков
ВЗЛОМ
zhukov@glc.ru

Александр «Dr.» Лозовский
MALWARE, КОДИНГ, PHREAKING
lozovsky@glc.ru

Юрий Гольцев
ВЗЛОМ
goltsev@glc.ru

Евгений Зобнин
X-MOBILE
zobnin@glc.ru

Илья Русанен
КОДИНГ
rusanen@glc.ru

Павел Круглов
UNIXOID и SYN/ACK
kruglov@glc.ru

MEGANEWS

Мария Нефёдова
nefedova.maria@gameland.ru

АРТ

Ирина Лободина
Верстальщик цифровой версии

Алик Вайнер
Обложка

РЕКЛАМА

Анна Яковлева
PR-менеджер
yakovleva.a@glc.ru

Мария Самсоненко
Менеджер по рекламе
samsonenko@glc.ru

РАСПРОСТРАНЕНИЕ И ПОДПИСКА

Подробная информация по подписке shop.glc.ru, info@glc.ru
Отдел распространения
Наталья Алехина (lapina@glc.ru)
Адрес для писем: Москва, 109147, а/я 50

В случае возникновения вопросов по качеству печати: claim@glc.ru. Адрес редакции: 115280, Москва, ул. Ленинская Слобода, д. 19, Омега плаза. Издатель: ООО «Эрсиа»: 606400, Нижегородская обл., Балахнинский р-н, г. Балахна, Советская пл., д. 13. Учредитель: ООО «Принтер Эдишионс», 614111, Пермский край, г. Пермь, ул. Яблочкова, д. 26. Зарегистрировано в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзоре), свидетельство ПИ № ФС77-56756 от 29.01.2014 года. Мнение редакции не обязательно совпадает с мнением авторов. Все материалы в номере предоставляются как информация к размышлению. Лица, использующие данную информацию в противозаконных целях, могут быть привлечены к ответственности. Редакция не несет ответственности за содержание рекламных объявлений в номере. По вопросам лицензирования и получения прав на использование редакционных материалов журнала обращайтесь по адресу: xakep@glc.ru. © Журнал «Хакер», РФ, 2015