Научно-исследовательская работа
Техническое творчество и изобретательство

ПРОВЕРКА ВОЗМОЖНОСТИ СОЗДАНИЯ УСТРОЙСТВА СКРЫТОГО УДАЛЁННОГО УПРАВЛЕНИЯ КОМПЬЮТЕРОМ С ПОМОЩЬЮ КОМПЬЮТЕРНОЙ МЫШИ

Выполнили:

Килимов Темирлан Русланович,
курсант 1-го курса
Каспийского института морского и речного транспорта
им. ген-адм. Ф. М. Апраксина – филиал ФГБОУ ВО «ВГУВТ»

Мостовой Александр Олегович,
курсант 1-го курса
Каспийского института морского и речного транспорта
им. ген-адм. Ф. М. Апраксина – филиал ФГБОУ ВО «ВГУВТ»

Лепский Владислав Александрович,
курсант 2-го курса
Каспийского института морского и речного транспорта
им. ген-адм. Ф. М. Апраксина – филиал ФГБОУ ВО «ВГУВТ»

Руководитель:

Ракин Григорий Валерьевич
к. п. н., доцент кафедры МиЕД
Каспийского института морского и речного транспорта
им. ген-адм. Ф. М. Апраксина – филиал ФГБОУ ВО «ВГУВТ»

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

«Кто владеет информацией, тот владеет миром!», – эти слова приписывают английскому банкиру и финансисту, а также члену одной из самых богатых семей Натану Ротшильду. На сегодняшний день, когда весь мир насквозь пронизан различными информационными сетями, позволяющими передавать информацию по всему миру буквально за секунды, эти слова являются наиболее актуальными. Ведь достоверная и своевременно полученная информация имеет большую ценность, чем золото и деньги.

Поэтому, если раньше «охотники за чужими деньгами», как правило, носили маски и использовали холодное или огнестрельное оружие, то теперь достаточно часто они пользуются компьютерами и интернетом, и другими устройствами, а находится при этом они могут на расстоянии тысячи километров от места ограбления. Их называют кибер-преступниками или хакерами. Недавний взлом криптобиржы Bybit, в результате которого было украдено порядка $1.4 млрд называют одним из самых масштабных киберпреступлений[1].

Причём в некоторых случаях потеря денег может быть самым безобидным последствием их деятельности[2]. Поэтому, работа специалистов по информационный безопасности, таких как пинтестеры или белые хакеры является очень актуальной.

Для того, чтобы успешно противостоять своему врагу, необходимо знать, его возможности и средства. Так, одной из приоритетных целей хакинга является получение полного удалённого доступа к системе. Для этого могут использоваться различные вредоносные программы (вирусы), а также уязвимости системы или программного кода, как например «backdoor».

---

[1] Коган Евгений. Как взломали Bybit // Новости фондового рынка, ценных бумаг и экономики, прогнозы и анализ – Финам.ру [Электронный ресурс]. Режим доступа: https://www.finam.ru/publications/item/kak-vzlomali-bybit-20250223-1604/ (дата обращения 28.02.2025).

[2] Владимир Тодоров. Ядерные черви. Как хакеры лишают людей электричества, парализуют больницы и атакуют АЭС // Lenta.ru – Новости России и мира сегодня [Электронный ресурс]. Режим доступа: https://lenta.ru/articles/2017/01/16/criticaldamage/ (дата обращения 28.02.2025).

Современные антивирусные программы, а также элементарные меры информационной профилактики во многом могут защитить от проникновения вредоносных программ на ваше устройство.

Но какую опасность может представлять обычная компьютерная мышь, не содержащая ни устройств хранения информации, ни имеющая выхода в интернет. Как оказалось, даже из обычной мыши можно сделать полноценное хакерское устройство.

ОПИСАНИЕ ИСПОЛЬЗУЕМОЙ ТЕХНОЛОГИИ

Основной частью разрабатываемого устройства будет является Raspberry Pi Zero W (рис. 1) [1]. Raspberry Pi Zero W – это миниатюрный одноплатный компьютер на базе SoC чипа Broadcom BCM2835, работающий на ОС Linux. Чип Broadcom BCM2835 включает в себя процессор CPU ARM1176JZ-F, разогнанный до частоты 1 ГГц, и двухъядерный графический процессор GPU VideoCore IV с частотой 400 МГц.

Рис. 1. Raspberry Pi Zero W

Главное отличие Raspberry Pi Zero W от стандартной Raspberry Pi Zero – наличие беспроводного модуля с Wi-Fi и Bluetooth, что позволяет интегрировать мини-компьютер в проекты интернета вещей (IoT) без дополнительной периферии. Мощности процессора хватает для работы с графическими операционными системами, воспроизведения фильмов, ретро-эмуляции и обработки потокового видео с помощью библиотеки OpenCV [2].

Для работы в специальный слот необходимо вставить карту памяти microSD, с заранее записанным дистрибутивом Raspbian на базе Linux или другой доступной системы (рис 2).

Рис. 2. Подготовка Raspberry Pi Zero W к работе

Но в нашем случае необходима специальное программное обеспечение или так называемая «прошивка» – P4WNP1, работающая под управление ОС Kali Linux. P4wnP1 — это настраиваемая платформа для атак через USB.

Возможности P4wnP1:

- Создание точки доступа по Wi-Fi для доступа по SSH (только Pi Zero W), поддержка скрытого ESSID.
- Работа с Wi-Fi в клиентском режиме (только Pi Zero W), чтобы передавать сетевые атаки через USB по Wi-Fi с доступом в Интернет (MitM)
- Работа с функциями USB-устройства в любой возможной комбинации с поддержкой подключения и воспроизведения в Windows (драйверы класса).

Поскольку P4wnP1 — это гибкий фреймворк, он позволяет получить пользователю полный доступ к компьютеру, ограниченный только его воображением.

СОЗДАНИЕ УСТРОЙСТВА СКРЫТОГО УДАЛЁННОГО ДОСТУПА С ПОМОЩЬЮ КОМПЬЮТЕРНОЙ МЫШИ

Если в Raspberry Pi Zero пометить MisroSD карту с предустановленной прошивкой P4wnP1, а затем соединить плату мыши и Raspberry Pi, спрятав всё это в корпусе мыши, то получается устройство скрытого управления компьютером (рис. 3.)

Рис. 3. Компьютерная мышь с вмонтированным в неё микрокомпьютером Raspberry PI Zero W

Данное устройство можно назвать «физическим компьютерным вирусом», который «можно потрогать».

Процесс подключения происходит следующим образом. Через USB-hub соединяются плата мыши, Raspberry PI Zero W и usb-кабель, второй конец которого подключается к компьютеру. Если знать ip-адрес включенного в сеть Raspberry PI, то достаточно легко можно осуществить подключение к нему с атакующего устройства (компьютера или смартфона) помощью программы *putti*. Подключение происходит с использованием технологии *ssh*.

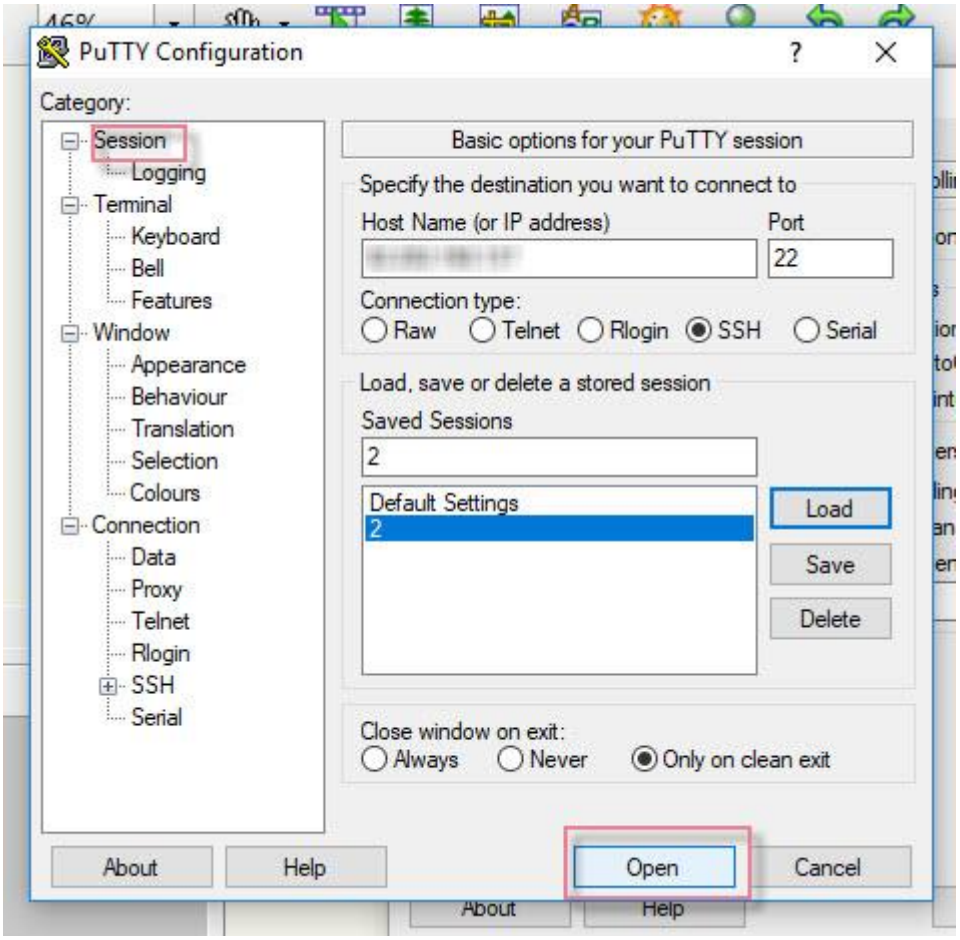

Рис. 4. Подключение к Raspberry PI с помощью программы *putty*

SSH (англ. *Secure Shell* — «безопасная оболочка») — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов). Схож по функциональности с протоколами *Telnet* и *rlogin*, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли. *SSH* допускает выбор различных алгоритмов шифрования. *SSH* позволяет безопасно передавать в незащищённой среде практически любой другой сетевой протокол. Таким образом, можно не только удалённо работать на компьютере через командную оболочку, но и передавать по шифрованному каналу звуковой поток или видео (например, с веб-камеры) [3].

После подключения такого устройства к компьютеру, компьютер становится «заряженным» – с атакующего устройства с помощью технологии *ssh* могут посылаться различные команды на Raspberry PI, с помощью которого

данные команды будут выполняться на атакуемом компьютере без ведома непосредственного пользователя, то есть атакующий получает полные права администратора над атакуемым компьютером, действуя при этом удалённо (рис. 5).

Рис. 5. Удалённое управление компьютером со смартфона

Необходимо отметить, что антивирусные программы никак не реагирует на данное устройство. Единственный признак скрытого проникновения в систему – появление в списке сетевых подключений сети «P4WNP1», причём данная сеть пропадает из списка при отключении «хакерского устройства» (рис 6).

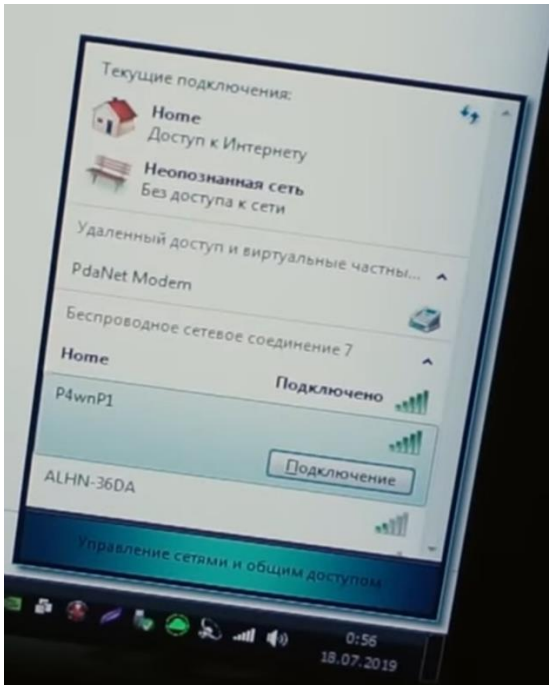

Рис. 6. Список беспроводных сетевых подключений на атакуемом устройстве

Одним из слабых мест данной технологии является то, что для осуществления атаки необходимо находиться в пределе Wi-Fi сигнала. Однако эту проблему также можно решить, если использовать иметь направленную антенну, но даже в этом случае с определённого расстояния сигнал Wi-Fi теряется.

ЗАКЛЮЧЕНИЕ

Технологии совершенствуются с каждым днём, а с учётом того, что невозможно представить нашу жизнь без информационных технологий, знание правил информационной безопасности должно стать таким же обязательным, как и знание правил безопасного обращения с огнём, электроприборами или правил дорожного движения.

В данной работе было показано, что даже абсолютно безопасное на первый взгляд периферийное устройство может нести скрытую опасность. Поэтому элементарная внимательность и соблюдение правил будет куда более надёжной защитой, чем самые современные антивирусные программы.

P. S. Желаем Вам безопасности ваших данных и бесплатного антивирусной программы со 100% эффективностью, которая при этом не будет перегружать систему Вашего компьютера.

СПИСОК ЛИТЕРАТУРЫ

1. Делаем USB-Backdoor из Raspberry Pi Zero W и P4wnP1 // форум информационной безопасности – Codeby.net [Электронный ресурс]. URL: https://codeby.net/threads/delayem-usb-backdoor-iz-raspberry-pi-zero-w-i-p4wnp1.66337/ (Дата обращения 19.02.2025).

2. Raspberry Pi Zero W, Одноплатный компьютер на базе 1-ядерного процессора 1ГГц // Чип и Дип – интернет магазин приборов и электронных компонентов [Электронный ресурс]. Режим доступа: https://www.chipdip.ru/product/raspberry-pi-zero-w (Дата обращения 28.02.2025).

3. SSH // Википедия – свободная энциклопедия [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/SSH (Дата обращения 28.02.2025).