Романов Д.Р. Эмуляция клавиатуры через USB RUBBER DUCKY: автоматизированное заражение без файлов // Международный журнал информационных технологий и энергоэффективности.– 2025. –Т. 10 № 3(53) с. 50–53

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ЭМУЛЯЦИЯ КЛАВИАТУРЫ ЧЕРЕЗ USB RUBBER DUCKY: АВТОМАТИЗИРОВАННОЕ ЗАРАЖЕНИЕ БЕЗ ФАЙЛОВ

Романов Д.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: danilio2003.dr@gmail.com

USB Rubber Ducky — это специализированное устройство, которое использует эмуляцию клавиатуры для выполнения вредоносных команд на целевой системе без необходимости установки файлов. В статье рассматривается принцип работы Rubber Ducky, механизмы автоматизированных атак, сценарии эксплуатации в реальной среде и методы защиты от подобных угроз. Особое внимание уделяется концепции fileless-атак, которые позволяют злоумышленникам обходить традиционные антивирусные решения и системы обнаружения вторжений.

Ключевые слова: USB Rubber Ducky, эмуляция клавиатуры, fileless-атака, автоматизированное заражение, безопасность, USB-угрозы, защита информации.

KEYBOARD EMULATION VIA USB RUBBER DUCKY: FILELESS AUTOMATED INFECTION

Romanov D.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: danilio2003.dr@gmail.com

USB Rubber Ducky is a specialized device that uses keyboard emulation to execute malicious commands on a target system without requiring file installation. This article explores the working principle of Rubber Ducky, mechanisms of automated attacks, real-world exploitation scenarios, and protection methods against such threats. Special attention is given to the concept of fileless attacks, which allow attackers to bypass traditional antivirus solutions and intrusion detection systems.

Keywords: USB Rubber Ducky, keyboard emulation, fileless attack, automated infection, cybersecurity, USB threats, information security.

Введение

В современном мире угрозы информационной безопасности становятся всё более изощрёнными, а методы атаки — сложнее и эффективнее. Одним из таких методов является использование устройств, эмулирующих клавиатуру, среди которых особенно выделяется USB Rubber Ducky. Этот инструмент, внешне напоминающий обычную флешку, позволяет злоумышленникам незаметно выполнять вредоносные команды на атакуемой системе. В отличие от традиционных вредоносных программ, USB Rubber Ducky не требует установки файлов на диск, а использует механизмы эмуляции клавиатуры для быстрого ввода команд, что делает атаку практически незаметной для антивирусных систем.

Концепция атаки на основе эмуляции клавиатуры основана на простом, но эффективном подходе: операционная система доверяет физическим устройствам ввода, таким как клавиатура, и практически не проверяет их на наличие вредоносных действий. Это позволяет Rubber Ducky автоматически вводить команды так, как если бы их печатал сам пользователь, но с гораздо большей скоростью и точностью. Такие атаки могут использоваться для кражи данных, установки бэкдоров, скачивания вредоносного ПО или даже отключения системной защиты.

С ростом популярности USB Rubber Ducky и аналогичных устройств актуальность защиты от подобных атак возрастает. Несмотря на опасность этой угрозы, многие организации и пользователи недооценивают риски, связанные с подключением незнакомых USB-устройств. В данной статье подробно рассматривается принцип работы USB Rubber Ducky, примеры его использования в атаках, а также методы защиты от подобных угроз.

Эмуляция клавиатуры через USB Rubber Ducky: автоматизированное заражение без файлов

USB Rubber Ducky — это устройство, созданное для автоматизированного выполнения команд на целевой машине. Оно использует эмуляцию клавиатуры, что позволяет выполнять любые команды с привилегиями пользователя, который в данный момент авторизован в системе. Устройство программируется с помощью специального языка сценариев Ducky Script, который позволяет задать последовательность команд, вводимых в систему. В отличие от обычной флешки, Rubber Ducky определяется компьютером не как USB-накопитель, а как HID (Human Interface Device), что делает его невидимым для стандартных систем безопасности[1].

Принцип работы Rubber Ducky довольно прост. Как только устройство подключается к компьютеру, оно мгновенно начинает вводить заранее подготовленные команды. Например, атакующий может запрограммировать Rubber Ducky на открытие командной строки (cmd.exe) и выполнение PowerShell-скрипта, который загружает вредоносный код из сети и выполняет его в памяти без записи на диск. Этот метод позволяет обходить большинство традиционных антивирусных решений, которые отслеживают файлы, но не анализируют ввод с клавиатуры[2].

Одним из самых популярных сценариев атаки является получение удалённого доступа через обратное подключение (reverse shell). Rubber Ducky может быстро ввести команду, которая подключает целевую машину к серверу атакующего, позволяя ему выполнять команды удалённо. Этот метод используется не только хакерами, но и тестировщиками на проникновение (pentesters) для оценки уровня безопасности организаций[3].

Другой вариант использования Rubber Ducky — кража паролей. Устройство может быстро открыть диспетчер учетных данных Windows или извлечь сохранённые пароли из браузеров, сохранив их в скрытом файле или отправив на сервер злоумышленника. Также возможны атаки на двухфакторную аутентификацию, когда Rubber Ducky перехватывает временные коды или автоматически вводит скомпрометированные данные на веб-сайтах[4].

Популярность Rubber Ducky объясняется не только его эффективностью, но и доступностью. Сценарии атак можно найти в открытых репозиториях, таких как GitHub, а само устройство легко купить или даже создать самостоятельно, используя

микроконтроллеры, такие как Digispark. Это делает подобные атаки потенциально опасными даже для обычных пользователей, не обладающих глубокими техническими знаниями.

Несмотря на высокую угрозу, существует ряд методов защиты от атак с использованием USB Rubber Ducky. Во-первых, рекомендуется ограничить использование USB-устройств с помощью групповых политик Windows или специализированных решений для контроля подключаемых периферийных устройств. Организации могут использовать программное обеспечение для мониторинга HID-устройств и отключения несанкционированных клавиатур[5].

Во-вторых, стоит настроить систему таким образом, чтобы любая новая клавиатура требовала ручного подтверждения перед активацией. Например, в некоторых Linux-дистрибутивах уже существуют механизмы, позволяющие блокировать автоматическое определение HID-устройств.

Третий важный аспект защиты — это осведомлённость пользователей. Часто атака начинается с физического доступа к устройству, когда злоумышленник незаметно подключает Rubber Ducky к компьютеру жертвы. Поэтому важно обучать сотрудников и пользователей не подключать неизвестные USB-устройства, даже если они выглядят как обычные флешки.

Дополнительно можно использовать специализированное программное обеспечение, такое как USBKill, которое отслеживает появление новых HID-устройств и может автоматически блокировать их, если они не были заранее одобрены пользователем. Также эффективным методом защиты является отключение PowerShell или ограничение его функций через групповые политики, что затруднит выполнение вредоносных команд.

Таким образом, атаки с использованием USB Rubber Ducky представляют серьёзную угрозу, так как позволяют автоматизировать выполнение команд без необходимости установки вредоносных файлов. Однако при правильной настройке систем безопасности и повышении осведомлённости пользователей можно значительно снизить риск успешной эксплуатации данной технологии.

Заключение

Эмуляция клавиатуры через USB Rubber Ducky является одним из наиболее эффективных методов атак, позволяющих обойти традиционные средства защиты и автоматизировать выполнение вредоносных команд. Этот инструмент активно используется как в целях тестирования безопасности, так и в реальных атаках, нацеленных на корпоративные сети и персональные компьютеры.

Главная опасность Rubber Ducky заключается в том, что он не требует установки вредоносных файлов и способен обходить традиционные антивирусные решения. Подобные атаки становятся всё более популярными, особенно с учётом доступности устройства и большого количества готовых сценариев в открытых источниках.

Для защиты от атак через USB Rubber Ducky необходимо применять комплексный подход: ограничение доступа к USB-портам, мониторинг HID-устройств, блокировка PowerShell и повышение осведомлённости пользователей. В условиях постоянно развивающихся угроз информационной безопасности осознание рисков и внедрение эффективных защитных механизмов являются ключевыми мерами для предотвращения подобных атак.

Список литературы

1. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
3. Чмутов М. В. и др. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре //Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. – 2017. – С. 535-537.
4. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.
5. Казанцев А. А., Прохоров М. В., Худякова П. С. Обзор подходов к классификации текстов актуальными методами //Экономика и качество систем связи. – 2021. – №. 1 (19). – С. 57-67.

References

1. Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data //High-tech technologies in Earth space research. 2020. – Vol. 12. – No. 1. – pp. 70-76.
2. Minyaev A. A. A method for evaluating the effectiveness of an information security system geographically distributed personal data information systems //Actual problems of infotelec communications in science and education (APINO 2020), 2020, pp. 716-719.
3. Chmutov M. V. and others. A study of the current IT infrastructure of an organization for the subsequent transition to a cloud architecture //Information security of the regions of Russia (IBRD-2017). Conference materials. 2017. pp. 535-537.
4. Petrova T. V. et al. Approaches to detecting an attacker's wireless access point on a local computer network //Regional Informatics (RI-2022). – 2022. – pp. 572-573.
5. Kazantsev A. A., Prokhorov M. V., Khudyakova P. S. Review of approaches to text classification by current methods //Economics and quality of communication systems. – 2021. – №. 1 (19). – pp. 57-67.