РЕФЕРАТ ПО ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вредоносные программы. Руткиты.

Заболотная Кристина Александровна

Содержание

# 1 Введение

1. Определение вредоносных программ В современном информационном обществе вредоносные программы представляют собой одну из самых серьезных угроз для компьютеров и сетей. Вредоносные программы, также известные как малварь (malware), включают в себя различные виды вредоносного программного обеспечения, целью которого является нанесение ущерба компьютерам, украденных данных или нарушение работы системы.
2. Значение информационной безопасности в современном мире В современном мире, где практически все аспекты нашей жизни перешли в цифровую форму, информационная безопасность становится ключевым вопросом. Защита конфиденциальности, целостности и доступности информации становится все более важной как для частных лиц, так и для организаций. Угрозы в виде вредоносных программ и руткитов могут привести к серьезным последствиям, таким как утечка конфиденциальных данных, потеря финансовых средств или даже нарушение национальной безопасности. Таким образом, понимание природы вредоносных программ и методов защиты от них является необходимым элементом обеспечения информационной безопасности в современном мире. В данном реферате мы рассмотрим основные аспекты вредоносных программ и руткитов, их воздействие на компьютерные системы и методы борьбы с ними.

# 2 Глава 1. Виды вредоносных программ

1. Вирусы Вирусы - это один из наиболее распространенных видов вредоносных программ, которые способны копировать себя и распространяться на другие файлы или системы. Вирусы могут наносить ущерб компьютеру, удалять файлы, шифровать данные или даже управлять системой без разрешения пользователя.
2. Троянские программы Троянские программы представляют собой вредоносное программное обеспечение, которое скрывается под видом полезной или необходимой программы. Как только троянская программа запущена на компьютере, она может выполнять различные вредоносные действия, такие как сбор конфиденциальной информации, установка других вредоносных программ или удаленное управление компьютером.
3. Черви Черви - это вредоносные программы, которые способны самостоятельно распространяться по сети без необходимости вмешательства пользователя. Черви могут использовать уязвимости в сетевых протоколах или программном обеспечении для заражения других компьютеров. Они могут нанести значительный ущерб, вызывая перегрузку сети или уничтожение данных.
4. Руткиты Руткиты - это особый тип вредоносных программ, которые скрывают свою активность от системного администратора или антивирусного ПО. Руткиты могут изменять работу операционной системы, скрывать процессы или файлы, и даже предоставлять злоумышленнику удаленный доступ к зараженному компьютеру. Из-за своей невидимости руткиты могут быть трудными для обнаружения и удаления. Руткиты - набор программных средств, обеспечивающих маскировку объектов, управление и сбор данных. Руткиты - программа, которая скрывает от антивирусов собственные действия, либо маскирует работу другого вредоносного ПО. Руткиты - вирусы, проникающие в компьютер различными нелегальными путями, предназначены для получения частичного или полного контроля над устройством.

# 3 Глава 2. Руткиты: определение и особенности

Руткиты представляют собой вредоносные программы, способные скрыть свою активность от системного администратора или антивирусных программ. Они получили свое название от слов “root” (корень) и “kit” (набор инструментов), так как они часто используются для получения привилегированного доступа к операционной системе и скрытия своего присутствия.

Основные особенности руткитов включают: 1. Невидимость: Руткиты могут скрывать свои процессы, файлы и сетевые соединения от стандартных средств мониторинга и обнаружения вредоносных программ. 2. Проникновение в ядро операционной системы: Некоторые руткиты могут модифицировать ядро операционной системы для обеспечения постоянного доступа и контроля над зараженным компьютером. 3. Устойчивость к удалению: Руткиты могут использовать различные методы для обеспечения своей выживаемости и устойчивости к удалению, например, перехват системных вызовов или защиту от записи на диск. Механизмы действия руткитов: Руткиты могут действовать по различным механизмам, включая: 1. Скрытие процессов и файлов: Руткиты могут скрывать свои процессы и файлы от стандартных инструментов мониторинга, что затрудняет обнаружение и удаление вредоносной программы. 2. Перехват системных вызовов: Руткиты могут перехватывать системные вызовы операционной системы, чтобы изменять и контролировать ее работу, например, для скрытия информации о своем присутствии. 3. Удаленное управление: Некоторые руткиты могут предоставлять злоумышленнику удаленный доступ и управление зараженным компьютером, что может использоваться для проведения кибератак или кражи конфиденциальной информации. Основные задачи руткитов: 1. Получить доступ к операционной системе с максимальными привилегиями: Руткиты стремятся получить полный контроль над зараженной системой, позволяя злоумышленникам выполнять различные действия без ведома пользователя. Это может включать удаленный доступ к системе, выполнение команд, сбор информации и многое другое. Руткиты могут обеспечить злоумышленникам возможность выполнения практически любых действий на зараженном компьютере. 2. Противодействие обнаружению: - Скрытие своего присутствия: Руткиты разработаны таким образом, чтобы быть максимально незаметными для пользователей и антивирусных программ. Они могут скрывать свои файлы, процессы и записи в системных журналах, чтобы избежать обнаружения. Это делает их удаление сложным процессом и позволяет руткитам продолжать свою деятельность на компьютере в течение длительного времени. - Затруднение обнаружения антивирусными программами: Руткиты используют различные методы для затруднения обнаружения антивирусными программами. Они могут изменять системные файлы и компоненты, маскироваться под легитимные процессы или использовать собственные методы шифрования и сокрытия. Это позволяет им избежать обнаружения и продолжать свою вредоносную деятельность. - Обход защитных механизмов: Руткиты могут обходить различные защитные механизмы, такие как файерволы и системы обнаружения вторжений. Они могут использовать уязвимости в операционной системе или программном обеспечении, чтобы получить доступ к системе, или использовать социальную инженерию для обмана пользователей и получения необходимых привилегий. Способы заражения руткитами: Руткиты могут быть распространены различными способами, включая: 1. Эксплуатация уязвимостей: Злоумышленники могут использовать уязвимости в операционной системе или приложениях для внедрения руткита на компьютер жертвы. 2. Социальная инженерия: Злоумышленники могут использовать методы социальной инженерии, такие как фишинговые письма или вредоносные веб-сайты, чтобы убедить пользователя установить руткит на свой компьютер. 3. Загрузка из недоверенных источников: Установка программного обеспечения из недоверенных источников или сомнительных сайтов может привести к заражению компьютера руткитом. Руткит опасен тем, что может измененять сетевой трафик на зараженной системе. Они могут перехватывать и изменять данные, передаваемые через сеть, что может привести к утечке конфиденциальной информации или выполнению нежелательных действий. Например, руткит может изменить адреса IP или DNS-записи, чтобы перенаправить пользователя на вредоносные веб-сайты или перехватить логин и пароль пользователя. Руткит может скрывать свои файлы и компоненты на зараженной системе. Они могут изменять атрибуты файлов или использовать скрытые папки и файлы, чтобы избежать обнаружения антивирусными программами или пользователями. Это делает удаление руткита сложным процессом, поскольку его файлы могут быть невидимыми и неотслеживаемыми. Руткиты могут иметь возможность обнаруживать и отключать антивирусные программы на зараженной системе. Они могут изменять системные файлы или процессы, связанные с антивирусным программным обеспечением, чтобы оно не могло работать правильно или вообще не запускалось. Это позволяет руткиту действовать незаметно и продолжать свою вредоносную деятельность без препятствий со стороны антивирусных программ.

Кто стоит за атаками? Учитывая весь спектр возможностей и сложности, связанные с разработкой руткитов, чаще всего их используют APT-группировки. Основной мотив злоумышленников такого уровня — получение данных, кибершпионаж. Например, Equation Group активно использовала руткит Flame в своих кибершпионских кампаниях на Ближнем Востоке. К слову, среди всех исследованных семейств руткитов в 77% случаев злоумышленники, распространяющие их, преследовали мотив получения данных. Примерно в трети случаев (31%) преступники стремились извлечь финансовую выгоду, как, например, Yingmob и TA505. Их атаки носили массовый характер и не были привязаны к конкретным отраслям, при этом Yingmob были нацелены на частных лиц. Самый редкий мотив — использование инфраструктуры компании-жертвы для проведения последующих атак. Он был отмечен лишь в 15% атак с использованием руткитов. В качестве основного способа распространения руткитов (85% случаев) злоумышленники используют методы социальной инженерии, такие как рассылка фишинговых сообщений, создание поддельных сайтов и приложений, имитирующих легитимные. Например, злоумышленники, распространяющие руткит Scranos, были ориентированы на частных лиц, поэтому в качестве способов распространения выбрали взломанное ПО и фишинговые рассылки. Анализ семейств руткитов показал, что в 44% случаев злоумышленники, используя эти вредоносы, атаковали госучреждения, чуть реже в качестве целей атак встречались учреждения науки и образования. Прежде всего это связано с основным мотивом, преследуемым преступниками, ведь информация, которая обрабатывается в организациях из этих отраслей, представляет большую ценность для злоумышленников. В атаках на финансовые организации применялось 19% руткитов. Один из примеров руткитов, ориентированных на банки, — Kronos. Его жертвами стали банки на территории Великобритании и Индии. Более половины руткитов (56%) используется и в атаках на частных лиц. Преимущественно это целенаправленные атаки в отношении высокопоставленных чиновников, дипломатов, сотрудников организаций, представляющих интерес для злоумышленников, то есть атаки в рамках кампаний по кибершпионаж.

# 4 Глава 3. Виды руткитов

Руткиты могут быть классифицированы по способу взаимодействия с операционной системой и уровню привилегий, которые они получают. Существуют следующие основные виды руткитов: 1. User-mode руткиты: Этот тип руткитов работает на уровне пользователя операционной системы и обычно использует методы перехвата системных вызовов для скрытия своей активности. User-mode руткиты могут скрывать процессы, файлы и реестр Windows, делая их невидимыми для стандартных инструментов мониторинга. 2. Kernel-mode руткиты: Kernel-mode руткиты оперируют на более низком уровне, имея прямой доступ к ядру операционной системы. Они могут модифицировать структуры данных ядра, перехватывать системные вызовы и контролировать работу операционной системы. Kernel-mode руткиты сложнее обнаружить и удалить, так как они имеют более высокие привилегии. 3. Bootkit руткиты: Bootkit руткиты заражают загрузочный сектор компьютера или загрузочный раздел диска, что позволяет им запускаться еще до загрузки операционной системы. Это делает их особенно опасными, так как они могут контролировать весь процесс загрузки компьютера и скрывать свою активность уже на этапе загрузки. Каждый из этих видов руткитов имеет свои особенности и методы работы, что делает необходимым комплексный подход к обнаружению и борьбе с этими вредоносными программами в рамках обеспечения информационной безопасности компьютерных систем.

# 5 Глава 4. Последствия заражения руткитами

Заражение компьютерной системы руткитом может иметь серьезные последствия для безопасности и функционирования информационной инфраструктуры. Ниже приведены основные последствия заражения руткитами: 1. Угроза конфиденциальности данных: Руткиты могут перехватывать и копировать конфиденциальную информацию, такую как личные данные пользователей, пароли, банковские реквизиты и другие чувствительные данные. Это создает риск утечки информации и нарушения конфиденциальности. 2. Угроза целостности системы: Руткиты могут изменять файловую систему, реестр Windows, ядро операционной системы и другие компоненты системы, что может привести к нарушению целостности и нормального функционирования компьютера. Это может привести к сбоям в работе программ, ошибкам в системе и потере данных. 3. Угроза доступности системы: Руткиты могут замедлить работу компьютера, вызвать зависания или полное отказ в доступе к системе. Они могут также блокировать доступ к антивирусным программам и другим инструментам безопасности, что делает обнаружение и удаление вредоносных программ более сложным. В целом, заражение руткитами представляет серьезную угрозу для информационной безопасности компьютерных систем и требует принятия мер по обнаружению, предотвращению и ликвидации этих вредоносных программ.

# 6 Глава 5. Способы защиты от руткитов

Для защиты компьютерных систем от руткитов необходимо применять комплексный подход, включающий следующие меры: 1. Использование антивирусных программ: Установка надежного антивирусного программного обеспечения поможет обнаружить и удалить руткиты на компьютере. Важно выбирать антивирус с функцией обнаружения скрытых угроз и регулярно обновлять его базы данных. 2. Регулярное обновление системы и программного обеспечения: Обновления операционной системы и установленных программ содержат исправления уязвимостей, которые могут быть использованы злоумышленниками для заражения руткитами. Поэтому важно следить за выходом новых версий и устанавливать их своевременно. 3. Ограничение прав доступа к системным ресурсам: Ограничение прав доступа пользователей к системным ресурсам поможет предотвратить установку и распространение руткитов. Рекомендуется использовать принцип минимальных привилегий, чтобы пользователи имели доступ только к необходимым для работы ресурсам. Применение этих мер поможет уменьшить риск заражения руткитами и обеспечить более высокий уровень информационной безопасности компьютерных систем.

# 7 Заключение

В заключение хочется подчеркнуть важность борьбы с вредоносными программами, включая руткиты. Руткиты представляют собой особую угрозу для компьютерных систем, поскольку они способны скрыть своё присутствие и действия от обычных пользователей и даже антивирусных программ. Это делает их особенно опасными для конфиденциальности и целостности данных. Так же, следует отметить, что руткиты имеют более совершенный бэкдор: Руткиты представляют собой более совершенный тип вредоносных программ, который может обеспечить злоумышленникам полный контроль над зараженной системой. Они могут действовать как бэкдоры, предоставляя злоумышленникам возможность удаленного доступа к системе, выполнения команд и сбора информации без ведома пользователя. Руткиты обладают способностью работать в системе очень длительное время, редко вызывая подозрения у пользователей или антивирусных программ. Они могут быть разработаны качественно и скрытно, что делает их обнаружение и удаление сложным процессом. Это позволяет злоумышленникам использовать руткиты для длительного шпионажа, кражи данных или других противоправных действий. Руткиты представляют собой сложнейшее испытание для средств защиты компьютерных систем. Из-за своей способности скрывать своё присутствие и действия, они могут обойти обычные методы обнаружения вредоносных программ. Это делает борьбу с руткитами сложной задачей для антивирусных программ, файерволов и других средств защиты. Для обеспечения информационной безопасности необходимо принимать меры по защите от руткитов и других вредоносных программ. Регулярное обновление антивирусного ПО, операционной системы и программного обеспечения, ограничение прав доступа пользователей к системным ресурсам – все это важные шаги в направлении обеспечения безопасности компьютерных систем.

# Список литературы

1. Скитович М. “Вредоносные программы: анализ и защита”, 2018.
2. Харлинг Д. “Руткиты: скрытые угрозы для компьютеров”, 2016.
3. Гудков А. “Основы информационной безопасности”, 2019.
4. Макаров Д. “Методы обнаружения и защиты от руткитов”, 2015.
5. https://www.ptsecurity.com/ru-ru/research/analytics/rootkits-evolution-and- detection-methods/
6. https://www.ptsecurity.com/ru-ru/research/analytics/rootkits-evolution-and- detection-methods