Долгушева А.В., Таран В.В., Чернова С.В. Исследование системы защиты от вредоносных программ и кибератак // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 8(34) с. 17–23

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

ИССЛЕДОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ И КИБЕРАТАК

Долгушева А.В., [1]Таран В.В., Чернова С.В.
ФГБОУ ВО "ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ", Самара, Россия (443010, Самарская область, город Самара,улица Льва Толстого, дом 23), e-mail: [1]kim.drive43@mail.ru

В данной статье рассматривается тема кибербезопасности и вирусов, какие угрозы существуют в интернете и какие меры безопасности необходимо принимать для защиты своих данных и личной информации. А также различные виды вирусов и их действия. Описывается, как вирусы попадают на компьютер, какие последствия они могут иметь и как защититься от них. Представлен список аскетов по исследование системы защиты от вредоносных программ и кибератак. В заключении подчеркивается важность защиты своих данных и личной информации в интернете, а также необходимость постоянного обновления мер безопасности для борьбы с угрозами кибербезопасности, распространенных во всем мире, и возможных способов их преодоления.

Ключевые слова: Кибератаки, вредоносные программы, система защиты.

INVESTIGATION OF THE SYSTEM OF PROTECTION AGAINST MALWARE AND CYBER ATTACKS

Dolgusheva A.V., [1]Taran V.V., Chernova S.V.
VOLGA STATE UNIVERSITY OF TELECOMMUNICATIONS AND INFORMATICS, Samara, Russia (443010, Samara region, Samara city, Leo Tolstoy street, 23), e-mail: [1]kim.drive43@mail.ru

This article discusses the topic of cybersecurity and viruses, what threats exist on the Internet and what security measures need to be taken to protect your data and personal information. As well as various types of viruses and their actions. It describes how viruses get on the computer, what consequences they can have and how to protect against them. The list of ascetics for the study of the system of protection against malware and cyber attacks is presented. The conclusion emphasizes the importance of protecting your data and personal information on the Internet, as well as the need for constant updating of security measures to combat cybersecurity threats common throughout the world, and possible ways to overcome them.

Keywords: Cyber attacks, malware, protection system.

Введение

Современный мир зависит от информационных технологий, и этот факт делает нас более уязвимыми к кибератакам и вирусам.

Кибератака — это попытка несанкционированного доступа к компьютерной системе, чтобы украсть, изменить или уничтожить данные. Кибератаки могут осуществляться с

помощью различных методов, таких как вирусы, троянские программы, фишинг и другие вредоносные действия.

Вирус — это программа, которая может копировать себя и распространяться на другие компьютеры. Вирусы могут привести к потере данных, нарушению работы компьютеров, краже личной информации и многим другим негативным последствиям. Вирусы могут распространяться через электронную почту, загрузки из Интернета, портативные устройства и другие способы.

Вирусной атакой, называется атака на удаленную/локальную компьютерную систему с использованием вредоносного программного обеспечения (вирусов). Они являются более изощренным методом доступа к секретной информации, поскольку хакеры используют специальные программы для работы на компьютере жертвы, а также для ее дальнейшего распространения (это вирусы и черви). Такие программы предназначены для поиска и передачи секретной информации своему владельцу или просто для повреждения системы безопасности и производительности компьютера жертвы. Принципы работы этих программ разные [1] .

Вредоносные программы и кибератаки

Вредоносные программы, также известные как малварь (malware), являются вредоносным программным обеспечением, разработанным для нанесения вреда компьютерным системам, сетям и пользователям. Они могут быть созданы злоумышленниками с различными целями, включая получение незаконного доступа к системе, кражу личных данных, финансовые мошенничества, шпионаж и прочие вредоносные действия.

Существует несколько типов вредоносных программ, включая:

Вирусы (Viruses): Это программы, которые могут размножаться и распространяться путем заражения других файлов или программ. Они прикрепляются к исполняемым файлам и могут внедряться в систему, повреждать файлы и распространяться на другие компьютеры через сети или носители информации.

Черви (Worms): Черви являются автономными программами, которые могут самостоятельно распространяться по компьютерным сетям. Они могут использовать уязвимости в сетевых протоколах или программном обеспечении для заражения компьютеров и их дальнейшего распространения [2].

Троянские программы (Trojans): Троянские программы скрываются под видом полезного или желаемого программного обеспечения, но при запуске выполняют вредоносные действия без ведома пользователя. Они могут открывать задние двери, собирать и передавать личные данные, создавать ботнеты и выполнять другие вредоносные функции.

Рекламное ПО (Adware): Рекламное программное обеспечение отображает навязчивую рекламу на компьютере пользователя. Оно может быть установлено с другими программами или распространяться через вредоносные сайты. Рекламное ПО может также собирать информацию о пользователе без его согласия.

Шпионское ПО (Spyware): Шпионское программное обеспечение отслеживает и собирает информацию о пользователе без его ведома и согласия. Оно может записывать

нажатия клавиш, отслеживать активность веб-браузера, собирать личные данные и передавать их злоумышленнику.

Кибератаки представляют собой злонамеренные действия, совершаемые в цифровом пространстве с целью нанести ущерб компьютерным системам, сетям или пользователям. Они могут быть осуществлены различными методами и иметь разные цели, включая кражу личных данных, финансовые мошенничества, нарушение работы систем, шпионаж и другие вредоносные действия.

Некоторые из распространенных типов кибератак включают:

Фишинг (Phishing): Это атака, при которой злоумышленник пытается обмануть пользователей, выдавая себя за надежное лицо или организацию. Целью фишинга является получение личных данных, таких как пароли, номера кредитных карт или банковские реквизиты.

Вредоносные программы (Malware): Как уже упоминалось ранее, вредоносные программы, такие как вирусы, черви, троянские программы и шпионское программное обеспечение, могут использоваться для целенаправленных атак на компьютерные системы, с целью нанести ущерб или получить несанкционированный доступ.

DDoS-атаки (Distributed Denial of Service): Это атаки, при которых злоумышленник пытается перегрузить целевую систему или сеть большим количеством запросов, что приводит к отказу в обслуживании для легитимных пользователей.

Взлом (Hacking): Взлом может быть направлен на получение несанкционированного доступа к компьютерной системе или сети, с целью кражи данных, изменения настроек или выполнения других вредоносных действий.

Социальная инженерия (Social Engineering): Это метод манипулирования людьми, чтобы получить доступ к конфиденциальной информации или выполнить действия, которые могут нанести ущерб. Примерами могут быть обман пользователей, чтобы получить их пароли, или убеждение сотрудников предоставить доступ к системе [3].

Способы защиты от вредоносных программ и кибератак

Существует несколько способов защиты от вредоносных программ:

1. Установка антивирусного программного обеспечения: Используйте надежное антивирусное программное обеспечение и регулярно обновляйте его. Антивирусное ПО поможет обнаружить и удалить вредоносные программы с вашего компьютера.

2. Обновление операционной системы и программ: Регулярно обновляйте операционную систему и все установленные программы. Обновления часто содержат исправления уязвимостей, которые могут быть использованы злоумышленниками для атак.

3. Осторожность при скачивании и установке программ: Загружайте программы только с надежных и официальных источников. Будьте внимательны при установке программ и не разрешайте им получать необходимые разрешения, если вы не уверены в их надежности.

4. Осмотрительность в интернете: Будьте осторожны при открытии вложений в электронных письмах, переходе по подозрительным ссылкам или скачивании файлов из ненадежных источников. Вредоносные программы могут быть скрыты в этих элементах.

5. Включение брандмауэра: Убедитесь, что брандмауэр на вашем компьютере включен. Брандмауэр помогает контролировать входящий и исходящий сетевой трафик и блокировать подозрительные соединения.

6. Резервное копирование данных: Регулярно создавайте резервные копии важных данных. В случае атаки или заражения вредоносной программой, резервные копии помогут восстановить информацию.

7. Обновление браузера и использование безопасного соединения: Обновляйте ваш браузер до последней версии и предпочитайте использование безопасного HTTPS-соединения при посещении веб-сайтов.

8. Обучение пользователей: Проводите обучение пользователей по базовым правилам безопасности, таким как неоткрывание подозрительных ссылок, нескачивание файлов из ненадежных источников и осмотрительность при взаимодействии с электронной почтой.

9. Многофакторная аутентификация: Включите многофакторную аутентификацию для важных аккаунтов. Это дополнительный слой защиты, требующий не только пароль, но и дополнительный фактор, такой как одноразовый код или отпечаток пальца.

10. Мониторинг и обнаружение угроз: Используйте программное обеспечение для мониторинга и обнаружения угроз, которое поможет выявить аномальную активность и своевременно предупредить о возможных атаках.

Все эти меры в комбинации могут помочь защитить вашу систему от вредоносных программ и повысить уровень безопасности [4-6].

Для защиты от кибератак существует ряд мер и методов. Вот несколько основных способов защиты:

1. Постоянное обновление программного обеспечения: Регулярно обновляйте операционную систему, приложения и программное обеспечение до последних версий. Обновления часто содержат исправления уязвимостей, которые могут быть использованы злоумышленниками для проведения атак.

2. Использование надежного антивирусного программного обеспечения: Установите и регулярно обновляйте антивирусное программное обеспечение на своем компьютере. Это поможет обнаруживать и блокировать вредоносные программы, включая программы-шпионы и троянские кони.

3. Файервол: Установите и настройте брандмауэр на своем компьютере или сетевом устройстве. Файервол поможет контролировать входящий и исходящий сетевой трафик и блокировать подозрительные соединения.

4. Сильные пароли и многофакторная аутентификация: Используйте сложные и уникальные пароли для своих онлайн-аккаунтов. Рекомендуется также включить многофакторную аутентификацию, чтобы требовать дополнительный фактор подтверждения, такой как одноразовый код, при входе в аккаунт.

5. Осмотрительность в интернете: Будьте внимательны при посещении веб-сайтов и открытии ссылок или вложений из ненадежных источников. Избегайте скачивания файлов с подозрительных сайтов и не предоставляйте личные данные на ненадежных веб-ресурсах.

6. Обучение пользователей: Обучите себя и других пользователям основным правилам безопасности в сети. Это может включать осведомленность о методах фишинга, социальной

инженерии и других видов кибератак, а также обучение о том, как реагировать и защищаться от них.

7. Регулярное резервное копирование данных: Регулярно создавайте резервные копии важных данных и храните их в надежном месте. Это поможет восстановить данные в случае утраты или шифрования в результате кибератаки.

8. Ограничение привилегий доступа: Ограничьте привилегии доступа пользователей и приложений на своем компьютере или сервере. Убедитесь, что только необходимые пользователи имеют доступ к конфиденциальной информации или системным ресурсам.

9. Мониторинг и обнаружение аномальной активности: Используйте специальное программное обеспечение для мониторинга и обнаружения аномалий в сети. Это поможет выявить подозрительную активность и своевременно предупредить о возможных кибератаках.

10. Регулярные аудиты и тестирование на проникновение: Проводите регулярные аудиты безопасности своей системы, а также тестирование на проникновение, чтобы выявить уязвимости и устранить их до того, как они могут быть использованы злоумышленниками.

Это лишь некоторые из основных способов защиты от кибератак. Важно постоянно быть внимательными и осведомленными о новых угрозах и методах защиты для эффективной борьбы с киберугрозами.

Исследование системы защиты от вредоносных программ и кибератак

Исследование системы защиты от вредоносных программ и кибератак является важным аспектом обеспечения информационной безопасности. Вот некоторые ключевые аспекты, которые могут быть включены в такое исследование:

- Угрозный анализ: Изучение существующих угроз и вредоносных программ, анализ их характеристик, методов распространения и воздействия на системы. Это позволит определить наиболее вероятные угрозы для вашей системы и разработать соответствующие контрмеры.
- Оценка уязвимостей: Исследование и анализ уязвимостей в вашей системе, которые могут быть использованы злоумышленниками для вторжения или проведения кибератак. Это включает оценку слабых мест в сетевой инфраструктуре, программном обеспечении, конфигурации систем и процедур безопасности.
- Анализ архитектуры защиты: Изучение текущей архитектуры защиты вашей системы, включая физические, сетевые и программные механизмы защиты. Оценка эффективности существующих мер защиты и их соответствие современным стандартам безопасности.
- Планирование и реализация мер безопасности: Разработка и реализация мер безопасности, направленных на защиту системы от вредоносных программ и кибератак. Это может включать обновление программного обеспечения, установку брандмауэров, антивирусных программ и других механизмов защиты, настройку систем мониторинга и регистрации событий, резервное копирование данных и регулярное обновление политик безопасности.
- Обучение и осведомленность пользователей: Разработка программ обучения пользователей по вопросам информационной безопасности, чтобы повысить их

осведомленность о потенциальных угрозах и о том, как следовать политикам и процедурам безопасности. Это может включать проведение тренингов, распространение информационных материалов и организацию регулярных проверок осведомленности.

- Мониторинг и обнаружение инцидентов: Разработка механизмов мониторинга и обнаружения инцидентов, которые позволят оперативно обнаружить и реагировать на потенциальные атаки и нарушения безопасности. Это включает настройку систем мониторинга сетевого трафика, анализ журналов событий, использование инструментов обнаружения вторжений и других методов обнаружения аномалий.
- Реагирование на инциденты: Разработка планов реагирования на инциденты и проведение учений по их исполнению. Это включает разработку процедур для обработки инцидентов, механизмов реагирования, координации сотрудников и взаимодействия с внешними экспертами по безопасности.

Важно отметить, что эти аспекты зависят от конкретных требований и особенностей вашей системы и должны быть адаптированы под ваши нужды. Рекомендуется также обратиться к специалистам в области информационной безопасности для получения более детальных рекомендаций и консультаций.

Заключение

Современный мир все больше зависит от информационных технологий, что делает нас более уязвимыми к кибератакам и вирусам. Поэтому понимание того, как работают вирусы и вредоносные программы, а также методы защиты от них, является крайне важным для обеспечения информационной безопасности и защиты личных данных.

В целом, защита от вирусов и вредоносных программ является актуальной проблемой в современном мире. Несмотря на то, что существует множество программ и методов, которые обеспечивают защиту, вирусы все равно находят способы проникновения в наши компьютеры и устройства. Важно быть внимательными и следить за своей информационной безопасностью, а также постоянно обновлять программное обеспечение и использовать антивирусные программы, чтобы минимизировать риски.

Список литературы

1. Вирусы и другие вредоносные программы // Национальный Открытый Университет-2017—URL: https://intuit.ru/studies/courses/76/76/lecture/27946(дата обращения: 26.06.2023)
2. 13 различных типов вредоносных программ // New-Science.ru—2021—URL: https://new-science.ru/13-razlichnyh-tipov-vredonosnyh-programm/(дата обращения: 26.06.2023)
3. Палаева Л. В. Основные виды кибератак на автоматизированные системы управления технологическим процессом и средства защиты от них / Л. В. Палаева, А. М. Хафизов, А. М. Гилязетдинова // Фундаментальные исследования.—2017.—10—С.507–511.
4. Алеексеев П. Антивирусы. Настраиваем защиту компьютера от вирусов / П. Алеексеев, Д. Козлов, Р. Прокди—Москва: Наука и Техника, 2018.—915 с.
5. Шаньгин В.Ф. Защита компьютерной информации / В.Ф. Шаньгин—Москва: ДМК Пресс, 2020.—544 с.

6. Александров К.П. Компьютер без сбоев, вирусов и проблем / К.П. Александров, Р.Г. Прокди—Москва: Наука и техника, 2017.—192 с.

References

1. Viruses and other malicious programs // National Open University. — 2017 — URL: https://intuit.ru/studies/courses/76/76/lecture/27946 (accessed: 06/26/2023)
2. 13 different types of malware // New-Science.ru . — 2021 — URL: https://new-science.ru/13-razlichnyh-tipov-vredonosnyh-programm / (accessed: 06/26/2023)
3. Palaeva L. V. NEW TYPES OF CYBERATTACKS ON AUTOMATED PROCESS CONTROL SYSTEMS AND MEANS OF PROTECTION AGAINST THEM / L. V. Palaeva, A.M. Hafizov, A.M. Gilyazetdinova // Fundamental research. — 2017. — 10. — pp. 507-511.
4. Aleekseev P. Antiviruses. Setting up computer protection against viruses / P. Aleekseev, D. Kozlov, R. Prokdi—Moscow: Science and Technology, 2018.—p.915
5. Shangin V.F. Protection of computer information / V.F. Shangin — Moscow: DMK Press, 2020.—p.544
6. Alexandrov K.P. Computer without failures, viruses and problems/K.P. Alexandrov, R.G. Prokdi—Moscow: Science and Technology, 2017.—p.192