DOI 10.36622/1682-7813.2024.27.1.005
УДК 004.056.57

СЕТЕВЫЕ АТАКИ КОМПЬЮТЕРНЫМИ ВИРУСАМИ: ЧАСТНЫЕ ИНСТРУКЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

О.Е. Кобцев, А.И. Шеншин, В.М. Питолин, В.И. Белоножкин, К.А. Разинкин, А.С. Кривошеин

Данная научная статья посвящена исследованию сетевых атак, осуществляемых компьютерными вирусами на корпоративные сети, в частности – разработке конкретных инструкций и рекомендаций по защите, адаптированных к практическому применению. В ходе исследования, на основе информации о сценариях (векторах) сетевых атак компьютерными вирусами, разработаны частные инструкции обеспечения информационной безопасности предприятия. Результаты исследования представляют собой вклад в обеспечение информационной безопасности предприятий, адаптированы для практического использования, а также могут служить основой для дальнейшей разработки мер по защите от сетевых атак компьютерными вирусами.

Ключевые слова: корпоративная сеть, компьютерные вирусы, уязвимости, частные инструкции.

Введение

Повсеместная информатизация и развитие технологий на сегодняшний день обуславливают значительное повышение эффективности множества процессов, включающих как повседневную активность частных лиц, так и масштабные бизнес-процессы организаций. При этом “обратной стороной” информатизации является появление новых угроз информационной безопасности, что усугубляется повышающейся зависимостью от информационных технологий. В этом контексте особенно выделяются сетевые атаки, осуществляемые с использованием компьютерных вирусов, наносящие значительный ущерб корпоративным сетям [1].

В современных условиях информатизации, рост количества и качества (расширения функционала) компьютерных вирусов и, следовательно, связанных с ними угроз безопасности корпоративных сетей является стойкой тенденцией, что обуславливает актуальность разработки мер по защите от соответствующих атак. Недостаточная защищенность корпоративных сетей коммерческих и государственных организаций может привести к серьезным последствиям, включая полную остановку бизнес-процессов, утечку конфиденциальных данных, отказ в обслуживании и подмену данных.

Исследование Positive Technologies за 2022 год выявило в 70% компаний высокую активность вредоносного программного обеспечения (ВПО) в корпоративных сетях [2], что обуславливает необходимость создания адекватного организационно-правового обеспечения защиты от вирусных атак.

Поэтому представленная работа направлена на исследование сетевых атак компьютерными вирусами на корпоративные сети и предлагает разработку частных инструкций безопасности информации, предназначенных для практического применения в рамках защиты информационных систем корпораций.

Векторы сетевых атак компьютерными вирусами

В рамках разработки частных инструкций информационной безопасности предприятия в контексте защиты от конкретного вида атак, необходимо проанализировать сценарии (векторы) соответствующей атаки. При этом необходимо придерживаться наиболее достоверных и проверенных источников. Основываясь на информации с ресурса capec.mitre.org [3], выделим пять уникальных сценариев атак, представленных в табл. 1.

Таблица 1

Векторы атак на приложения [3]

Атаки	Векторы атаки	Описание
Атака с помощью стелс-вирусов (VA_1)	Проникновение в систему через сетевой периметр	Использование стелс-вируса для обхода сетевых механизмов безопасности и проникновения в корпоративную сеть через уязвимости в сетевом периметре.
	Обход механизмов обнаружения и защиты	Обход механизмов обнаружения, таких как антивирусные программы, межсетевые экраны и системы обнаружения вторжений.
	Получение повышенных привилегий	Нацеленность на получение повышенных привилегий для обхода ограничений безопасности.
	Развитие атаки на целевые системы и реализация недопустимых событий	Продолжение развития атаки на целевые системы с использованием внутренних механизмов распространения и инфицирования.
	Получение доступа к ключевым системам	Использование стелс-вируса для получения доступа к ключевым системам в корпоративной сети.
	Установка задней двери	Установка задней двери для получения удаленного доступа и контроля над зараженной машиной или корпоративной сетью.
Атака с использованием макровирусов (VA_2)	Введение вредоносных макросов	Внедрение вредоносных макросов в документы и использование макроязыка для запуска вредоносного кода.
	Использование социальной инженерии	Использование социальной инженерии для убеждения пользователей в активации макросов и запуске вредоносного кода.
	Распространение через документы и сеть	Распространение макровирусов через зараженные документы, электронную почту, файлообменные сервисы и внутренние сетевые ресурсы.
	Маскировка и обход защитных механизмов	Маскировка макровирусов под легитимные макросы и обход антивирусных программ и других защитных механизмов.
	Запуск вредоносного кода	Запуск вредоносного кода при активации макросов, внедренных в макровирусе.
	Использование обновлений и патчей	Поиск уязвимостей в системах, приложениях и операционных системах для эксплуатации через макровирусы.
Атака с помощью сетевого червя (VA_3)	Идентификация уязвимых хостов	Поиск хостов в корпоративной сети с известными уязвимостями и слабыми местами в безопасности с использованием сканеров уязвимостей или автоматизированных инструментов.
	Эксплуатация уязвимостей	Использование уязвимостей в операционных системах, службах или приложениях на целевых хостах для получения несанкционированного доступа.

Продолжение табл. 1

Атаки	Векторы атаки	Описание
	Заражение хостов	Размещение червя на зараженных хостах и использование различных методов для распространения, включая слабые пароли, вредоносные вложения в электронных письмах или сетевые уязвимости.
	Автоматическое распространение	Автоматическое исследование сети червем, обнаружение других уязвимых хостов и попытка распространения без взаимодействия пользователя.
	Загрузка дополнительных компонентов	Загрузка дополнительных вредоносных компонентов на зараженные хосты для дальнейшей эксплуатации или вредоносных действий.
	Создание задней двери	Создание задней двери на зараженных хостах для получения удаленного доступа и управления системами в дальнейшем.
Атака вирус-ботнетом (VA_4)	Заражение устройств	Распространение вируса-ботнета через вредоносные вложения в электронных письмах, зараженные ссылки, загрузки или эксплуатацию уязвимостей.
	Маскировка и уклонение от обнаружения	Использование различных методов для маскировки активности и уклонения от обнаружения, включая шифрование команд и данных, изменение сетевого трафика.
	Распространение	Распространение вируса-ботнета на другие устройства внутри или вне корпоративной сети, используя эксплуатацию уязвимостей, сканирование сети и другие методы.
	Установка контрольного узла	Установка контрольного узла вирусом-ботнетом, который служит злоумышленнику для удаленного управления зараженными устройствами.
	Формирование ботнета	Превращение зараженных устройств в "боты", которые подчиняются командам и контролю злоумышленника.
	Команды и управление	Отправка команд ботнету через контрольный узел для выполнения различных задач, таких как DDoS-атаки, спам, кража данных и другие вредоносные действия.
Атака вирусом с функцией рекламного ПО (VA_5)	Внедрение вредоносного кода в рекламные баннеры	Внедрение вредоносного кода в рекламные баннеры на веб-сайтах в корпоративной сети. При загрузке баннера пользователь может быть заражен вредоносным кодом.
	Распространение через вредоносные рекламные элементы	Использование вредоносных рекламных баннеров или всплывающих окон для распространения вируса с функцией рекламного ПО.

Продолжение табл. 1

Атаки	Векторы атаки	Описание
	Использование эксплойтов и уязвимостей	Использование известных эксплойтов и уязвимостей в программном обеспечении, используемом в корпоративной сети, для внедрения вируса с функцией рекламного ПО.
	Маскировка под легитимное рекламное ПО	Маскировка вируса с функцией рекламного ПО под легитимное рекламное ПО или расширение браузера для избежания обнаружения.
	Нежелательное отображение рекламы	Навязчивое отображение рекламных материалов на компьютере пользователя в корпоративной сети.
	Кража данных	Сбор и передача конфиденциальной информации о пользователях, такой как персональные данные, приватные файлы или учетные данные.

В данном исследовании рассматриваются векторы атак, представленные в табл. 1. Они будут использоваться в качестве исходных данных в части механизмов реализации угрозы для формирования частной политики и регламентов информационной безопасности предприятия.

Частные инструкции обеспечения информационной безопасности

Сетевая безопасность является неотъемлемой частью современного бизнеса, и обеспечение защиты сети от различных векторов сетевых атак компьютерными вирусами она требует определенных функциональных знаний и навыков у администратора. Ниже в табл. 2 приведен перечень требований, к знаниям и умениям администратора, которыми он должен обладать, чтобы успешно защитить сеть организации.

Таблица 2

Умения и знаний Администратора при защите от сетевой атаки компьютерными вирусами

Функциональные знания Администратора, которыми он должен обладать, чтобы успешно защитить сеть Организации	Требования к умениям Администратора, которыми он должен владеть, чтобы успешно защищать сеть Организации
1	2
Атака с помощью стелс-вирусов (VA_1)	
Глубокое понимание алгоритмов шифрования и дешифрования для обнаружения и расшифровки зашифрованного вредоносного кода.	Умение анализировать поведение стелс-вирусов и обнаруживать скрытые аномалии в системе.
Знание методов и средств для мониторинга сетевого трафика и обнаружения необычных активностей, связанных с проникновением через сетевой периметр.	Умение настраивать системы мониторинга сетевого трафика, такие как Wireshark или Snort, и анализировать сетевые события для обнаружения потенциальных угроз.
Знание методов защиты от классического переполнения буфера, таких как использование механизмов проверки границ, буферизации и очистки входных данных.	Умение настраивать механизмы безопасности на уровне операционной системы и приложений, таких как Address Sanitizer или Buffer Overflow Protection.

Продолжение табл. 2

1	2
Понимание принципов работы аутентификации и авторизации, включая механизмы многофакторной аутентификации и принципы настройки прав доступа.	Умение настраивать и администрировать системы аутентификации и авторизации, такие как Active Directory или LDAP, включая использование механизмов многофакторной аутентификации.
Атака с использованием макровирусов (VA_2)	
Знание основ макросов в приложениях Microsoft Office и других популярных офисных пакетах.	Умение анализировать и оценивать макросы в документах на предмет наличия вредоносного кода и потенциальных уязвимостей, используя инструменты, такие как OfficeMalScanner или oledump.
Понимание принципов работы механизмов обнаружения и блокировки макровирусов, таких как системы антивирусной защиты и системы предотвращения внедрения.	Умение настраивать и поддерживать системы антивирусной защиты, обнаружения и блокировки макровирусов, такие как Symantec Endpoint Protection или McAfee Endpoint Security.
Знание методов контроля и управления доступом к макросам и ограничений выполнения макросов в офисных приложениях.	Умение настраивать политики безопасности в офисных приложениях для ограничения выполнения макросов и предотвращения вредоносных действий.
Атака с помощью сетевого червя (VA_3)	
Знание принципов работы сетевых протоколов и структуры пакетов для обнаружения и анализа сетевых атак, связанных с червями.	Умение настраивать системы обнаружения и предотвращения сетевых червей, включая системы интранет-детекции и системы межсетевой безопасности, такие как Snort или Cisco Firepower.
Понимание методов эксплуатации уязвимостей сетевых сервисов и принципов обхода механизмов аутентификации и авторизации.	Умение настраивать и администрировать сетевые сервисы с учетом принципов безопасности, включая использование инструментов, таких как Nmap или Metasploit.
Атака вирус-ботнетом (VA_4)	
Знание принципов функционирования вирусов-ботнетов и их механизмов управления.	Умение настраивать и поддерживать системы обнаружения и предотвращения ботнетов, включая системы обнаружения вторжений и межсетевой безопасности, такие как Intrusion Detection System (IDS) или Cisco ASA.
Понимание методов скрытого коммуникационного протоколирования и механизмов управления ботами.	Умение анализировать сетевой трафик для обнаружения подозрительной активности, связанной с ботнетами, и принимать меры по блокированию коммуникации и управления ботами.
Понимание методов анализа и обнаружения подозрительной активности, связанной с вирусами-ботнетами.	
Атака вирусом с функцией рекламного ПО (VA_5)	
Знание методов внедрения вредоносного кода в рекламные баннеры и механизмов маскировки под легитимное рекламное ПО.	Умение анализировать и идентифицировать вирусы с функцией рекламного ПО, включая использование антивирусных программ, таких как Kaspersky Anti-Virus, Norton AntiVirus, и инструментов анализа кода, например, IDA Pro и Ghidra.

Окончание табл. 2

1	2
Понимание методов защиты от уязвимостей, связанных с повышением привилегий и обходом механизмов аутентификации и авторизации.	Умение настраивать системы защиты от нежелательной рекламы, включая использование рекламных блокировщиков, таких как uBlock Origin и AdGuard, и сетевых экраниров, например, pfSense и Cisco ASA.
Знание методов обнаружения и предотвращения утечки конфиденциальной информации через рекламные баннеры и механизмы сбора данных.	

Полномочия Администратора представляют собой широкий спектр ответственности и возможностей в области безопасности корпоративных сетей. Администратор является ключевым фигурантом в обеспечении защиты информационных ресурсов сетевой инфраструктуры организации. Представленная ниже табл. 3 содержит перечень рекомендаций по настройке параметров средств защиты информации, необходимых для успешной защиты сети организации.

Таблица 3

Пример плана действий Администратора при выборе и настройке СЗИ [4]

Требование к защите информации от атаки компьютерными вирусами	Средство защиты информации, обеспечивающие выполнение данных требований	Рекомендация по настройке параметров средств защиты информации
1	2	3
Атака с помощью стелс-вирусов (VA_1)		
• Настройте и сконфигурируйте IDS и IPS согласно спецификации и требованиям вашей сетевой инфраструктуры • Постоянно отслеживайте и анализируйте события и уведомления, полученные от IDS и IPS. Будьте готовы к реагированию на возможные вторжения и атаки, и принимайте соответствующие меры по предотвращению угроз.	СЗИ от Kaspersky Endpoint Security	Рекомендуется настроить компонент "Предотвращение вторжений" в системе защиты информации
Атака с использованием макровирусов (VA_2)		
• Установите и настройте систему контроля и фильтрации содержимого электронной почты и файлов • Настройте правила фильтрации • Мониторьте и анализируйте журналы системы контроля и фильтрации для выявления потенциальных угроз	СЗИ от Kaspersky Endpoint Security	Рекомендуется настроить компонент "Защита от почтовых угроз" в системе защиты информации

Продолжение табл. 3

1	2	3
Атака с помощью сетевого червя (VA_3)		
• Необходимо обеспечить постоянное мониторинговое покрытие для всех сетевых узлов и серверов организации • Регулярно обновлять и проверять эффективность используемых сигнатур и правил обнаружения, чтобы быть в курсе новых видов атак • Вести регулярный мониторинг и аудит системы мониторинга и анализа событий для обнаружения и устранения возможных уязвимостей	СЗИ от Kaspersky Endpoint Security	Рекомендуется настроить компонент "Анализ поведения" в системе защиты информации
Атака вирус-ботнетом (VA_4)		
• Активировать и настроить компонент адаптивного контроля аномалий для обнаружения и блокировки аномальной активности • Обновлять базы данных компонента регулярно для эффективной защиты от новых видов вирусов • Мониторинг результатов работы компонента для обнаружения и принятия мер в случае атаки.	СЗИ от Kaspersky Endpoint Security	Рекомендуется настроить компонент "Адаптивный контроль аномалий" в системе защиты информации
Атака вирусом с функцией рекламного ПО (VA_5)		
• Определите требования безопасности информации, включая уровень конфиденциальности, целостности и доступности. • Идентифицируйте критически важные данные и системы, которые требуют защиты от атак с помощью вирусов, рекламного ПО и других угроз.	СЗИ от Kaspersky Endpoint Security	Рекомендуется настроить компонент "Защита от веб-угроз" в системе защиты информации

Разграничительная матрица является важным аспектом информационной безопасности, который направлен на обеспечение контроля и ограничения доступа к ресурсам системы. Она является структурой, определяющей права доступа для различных пользователей и групп пользователей на основе принципа наименьших привилегий [5].

Целью разграничительной матрицы в табл. 4 является создание эффективной системы управления доступом, которая гарантирует, что пользователи получают только необходимые права доступа для

выполнения своих задач, и избыточные привилегии ограничиваются. Это способствует обеспечению безопасности и защите конфиденциальной информации от несанкционированного доступа и злоупотребления привилегиями.

Таблица 4

Пример разграничительной матрицы доступа

Объекты защиты	Роли пользователей		
	Администратор	Внутренний пользователь	Внешний пользователь
Компьютеры и серверы	Полный доступ	Полный доступ	Доступ запрещен
Центральные системы управления доступом	Полный доступ	Доступ запрещен	Доступ запрещен
Веб-серверы Базы данных	Полный доступ	Ограниченный доступ (разрешено чтение баз данных)	Доступ запрещен
Системы с описанием мониторинга и журналирования событий	Полный доступ	Ограниченный доступ (разрешена запись и чтение логов событий)	Доступ запрещен
Электронная почта и почтовый клиент	Полный доступ	Полный доступ	Полный доступ
Периметр сети и сетевые устройства	Полный доступ	Ограниченный доступ (разрешено чтение конфигураций, и настройка правил)	Ограниченный доступ (разрешено чтение конфигурации)
Файловые серверы и широкополосные сети	Полный доступ	Полный доступ	Ограниченный доступ: (разрешено чтение файлов)
Корпоративные системы и программное обеспечение	Полный доступ	Ограниченный доступ (разрешено чтение и запись настроек системы)	Доступ запрещен
Сетевое оборудование Сетевые службы	Полный доступ	Ограниченный доступ (разрешено чтение конфигурации оборудования)	Доступ запрещен
Операционные системы и приложения	Полный доступ	Ограниченный доступ (разрешена чтение конфигурации и настроек системы)	Доступ запрещен
Компьютеры и серверы Мобильные устройства	Полный доступ	Полный доступ	Ограниченный доступ (разрешено чтение устройства)

В целях предотвращения сетевых атак, осуществляемых путем распространения компьютерных вирусов, пользователю рекомендуется соблюдать следующие требования:

– реализуйте принцип наименьших привилегий, предоставляя пользователям только необходимые права доступа к системам и данным,

− проверяйте и используйте лицензированное программное обеспечение и официальные приложения из надежных источников, чтобы минимизировать риск инфицирования компьютерными вирусами,

− устанавливайте обновления и патчи операционной системы и приложений своевременно, чтобы закрыть известные уязвимости и предотвратить несанкционированный доступ к системам,

− будьте внимательны при взаимодействии с электронными письмами, особенно с вложениями и ссылками, и избегайте открытия ненадежных и непроверенных источников, чтобы предотвратить внедрение вредоносных программ,

− обеспечьте безопасность сетевых соединений, используя только доверенные Wi-Fi сети и виртуальные частные сети (VPN), чтобы защитить свои данные от перехвата и несанкционированного доступа,

− установите и настройте антивирусное программное обеспечение и систему обнаружения вторжений (IDS) [6] на своих устройствах, и регулярно обновляйте их, чтобы обеспечить оптимальную защиту от известных и новых угроз,

− будьте осмотрительны при использовании внешних устройств, таких как USB-флешки, и избегайте подключения неизвестных и непроверенных устройств к компьютерам, чтобы предотвратить внедрение вредоносного кода и компрометацию системы.

Также необходимо отметить, что значительное внимание следует уделять повышению уровня информационной грамотности сотрудников в области безопасности, поскольку это является важным фактором в общем снижении рисков.

Осведомленные и обученные сотрудники способны более эффективно применять описанные выше меры защиты, что значительно сокращает вероятность успешной реализации векторов атак, представленных в таблице 1. Постоянное обновление знаний и обучение персонала в области информационной безопасности становятся неотъемлемой частью комплексной стратегии защиты предприятия от сетевых атак компьютерными вирусами.

Заключение

В ходе исследования были разработаны частные инструкции, адаптированные для обеспечения информационной безопасности корпоративных сетей в рамках защиты от сетевых атак компьютерными вирусами. Полученные инструкции представляют собой конкретные рекомендации и примеры, позволяющие эффективно защищать корпоративные сети от рассматриваемого вида атак. Стоит отметить, что следование предложенному формату и плану действий Администратора сети позволяет значительно снизить потенциальный ущерб от сетевых атак компьютерными вирусами. Предложенная в исследовании матрица доступа, в свою очередь, позволяет построить оптимальную схему разграничения доступа в контексте рассматриваемых векторов атак.

Таким образом, в ходе исследования были получены значимые результаты, в первую очередь с практической точки зрения. Они представляют собой набор требований к персоналу и специально адаптированных инструкций, позволяющих качественно повысить защищённость корпоративной сети предприятия.

Список литературы

1. Кибератаки. URL: https://www.tadviser.ru/index.php/Статья:Кибератаки (дата обращения 09.02.2024).

2. Обнаружение распространенных угроз ИБ в сетевом трафике. URL: https://www.ptsecurity.com/ru-ru/research/analytics/network-traffic-analysis-2022/ (дата обращения 09.02.2024).

3. Common Attack Pattern Enumeration and Classification. URL: https://capec.mitre.org.

4. Kaspersky Endpoint Security for Windows Help. URL: https://support.kaspersky.com/KESWin/12.1/en-US/222859.htm (дата обращения 09.02.2024).

5. Матрица доступа. URL: https://innostage-group.ru/solutions/infosecurity/access-matrix/ (дата обращения 09.02.2024).

6. Система обнаружения вторжений. URL: https://ru.wikipedia.org/wiki/Система_обнаружения_вторжений (дата обращения 09.02.2024).

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 14.02.2024

Информация об авторах

Кобцев Олег Евгеньевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Шеншин Александр Игоревич – аспирант, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Питолин Владимир Михайлович – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Белоножкин Владимир Иванович – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Разинкин Константин Александрович – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Кривошеин Александр Сергеевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

NETWORK ATTACKS BY COMPUTER VIRUSES: SPECIFIC INFORMATION SECURITY INSTRUCTIONS

O.E. Kobcev, A.I. Shenshin, V.M. Pitolin, V.I. Belonozhkin, K.A. Razinkin, A.S. Krivoshein

This scientific article is dedicated to the study of network attacks carried out by computer viruses on corporate networks, specifically focusing on the development of specific guidelines and recommendations for protection, adapted for practical use. During the research, based on information about scenarios (vectors) of network attacks by computer viruses, specific instructions for ensuring the information security of the enterprise were developed. The research results represent a contribution to ensuring the information security of enterprises, are adapted for practical use, and can serve as a basis for further development of measures to protect against network attacks by computer viruses.

Keywords: corporate network, computer viruses, vulnerabilities, risk landscape, private policy.

Submitted 14.02.2024

Information about the authors

Oleg E. Kobcev – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Alexander I. Shenshin – post-graduate, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Vladimir M. Pitolin – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Vladimir I. Belonozhkin – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Konstantin A. Razinkin – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Alexander S. Krivoshein – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com