Лекция 3: Вредоносное ПО

Тема: Вредоносное ПО и социальная инженерия

Технический университет Молдовы

Лектор: Максим Масютин

Введение

Здравствуйте. Сегодня мы погружаемся в мир вредоносного программного обеспечения, широко известного как вредоносное ПО. Это одна из наиболее динамичных областей кибербезопасности, в которой ежедневно появляются новые угрозы, а злоумышленники постоянно совершенствуют свои методы.

Позвольте начать с нескольких цифр, иллюстрирующих масштаб проблемы.

В 2025 году по всему миру было зафиксировано более 783 миллионов попыток атак программ-вымогателей, по сравнению с 658 миллионами в 2024 году. Прогнозы на 2026 год указывают на то, что это число может превысить один миллиард попыток. И программы-вымогатели — это лишь один из видов вредоносного ПО.

Компания Cyble зафиксировала в 2025 году 57 новых группировок, использующих программы-вымогатели, и 27 новых группировок, занимающихся вымогательством, а также более 350 новых штаммов программ-вымогателей. Экосистема вредоносного ПО обширна, изощрённа и чрезвычайно прибыльна для преступников. Понимание принципов работы вредоносного ПО необходимо для обеспечения защиты от него.

Часть 1: Таксономия вредоносного ПО

Вредоносное ПО — это любое программное обеспечение, умышленно созданное для нанесения ущерба компьютеру, серверу, сети или пользователю.

Английский термин "malware" образован от слов "malicious" (вредоносный) и "software" (программное обеспечение). Рассмотрим основные категории.

Вирусы

Вирус — это вредоносное ПО, которое прикрепляется к легитимной программе или файлу и распространяется при запуске этой программы. Подобно

биологическим вирусам, компьютерные вирусы не способны распространяться без носителя.

Характеристики:

- Для распространения требуется действие пользователя (запуск заражённой программы);
- Прикрепляется к легитимным файлам;
- Может повреждать или изменять файлы;
- Распространяется через заражённые носители, вложения электронной почты, загрузки.

Типы вирусов:

- **Файловые вирусы**: прикрепляются к исполняемым файлам
- **Вирусы загрузочного сектора**: заражают главную загрузочную запись
- **Макровирусы**: скрываются в макросах документов (Word, Excel)
- **Полиморфные вирусы**: изменяют свой код для уклонения от обнаружения
- **Метаморфные вирусы**: полностью перезаписывают самих себя

Историческая справка

Вирусы доминировали в 1990-х и начале 2000-х годов, однако стали менее распространены по мере того, как другие типы вредоносного ПО оказались более эффективными для злоумышленников.

Черви

Червь — это самовоспроизводящееся вредоносное ПО, которое автоматически распространяется по сетям, не требуя действий пользователя или программы-носителя. Это делает червей особенно опасными, поскольку они способны распространяться чрезвычайно быстро.

Характеристики:

- Самовоспроизводящийся
- Автоматически распространяется по сети
- Не требует программы-носителя
- Может потреблять пропускную способность сети и системные ресурсы
- Часто использует уязвимости для распространения

Известные примеры:

- **Червь Морриса (1988)**: один из первых червей, вывел из строя 10% подключённых к интернету компьютеров

- **Code Red (2001)**: использовал уязвимость IIS, заразил 359 000 компьютеров за 14 часов
- **SQL Slammer (2003)**: заразил 75 000 серверов за 10 минут
- **Conficker (2008)**: заразил миллионы компьютеров, активен до сих пор
- **WannaCry (2017)**: объединил механизм распространения червя с полезной нагрузкой программы-вымогателя

Трояны

Троян (или троянский конь) — это вредоносное ПО, замаскированное под легитимное программное обеспечение. Пользователей обманом заставляют установить его, полагая, что они получают полезную программу.

Название происходит от греческого мифа, в котором воины спрятались внутри деревянного коня, чтобы проникнуть в Трою. Трояны выглядят безвредными, но содержат скрытый вредоносный функционал.

Характеристики:

- Замаскирован под легитимное ПО
- Требует установки пользователем
- Не самовоспроизводится
- Часто обеспечивает доступ через лазейку (бэкдор)
- Может обладать функциональностью, выглядящей легитимной

Типы троянов:

- **Трояны удалённого доступа (RAT)**: предоставляют злоумышленникам удалённое управление
- **Банковские трояны**: похищают финансовые учётные данные
- **Трояны-загрузчики**: загружают дополнительное вредоносное ПО
- **Трояны-шпионы**: отслеживают активность пользователя
- **Трояны для кражи игровых аккаунтов**: похищают учётные данные игровых аккаунтов

Программы-вымогатели

Программа-вымогатель шифрует файлы жертвы или блокирует системы, требуя оплату (обычно в криптовалюте) за восстановление. В последние годы этот тип угроз стал доминирующим среди вредоносного ПО.

Характеристики:

- Шифрует файлы или блокирует системы

- Требует выкуп
- Часто использует стойкое шифрование
- Может устанавливать ограниченные сроки для оплаты
- Всё чаще нацелены на организации, а не на отдельных пользователей

Эволюция программ-вымогателей:

- **Ранние программы-вымогатели**: простые блокировщики экрана
- **CryptoLocker (2013)**: первая широко успешная программа-вымогатель с шифрованием
- **Двойное вымогательство (с 2019 г.)**: кража данных перед шифрованием, угроза публикации
- **Тройное вымогательство**: добавление DDoS-атак или обращение к клиентам жертвы
- **Вымогательство как услуга**: криминальная бизнес-модель

Статистика вызывает тревогу: число публично зафиксированных атак программ-вымогателей выросло до 7 200 в 2025 году по сравнению с 4 900 в 2024 году, что составляет увеличение на 47 процентов. Более 60 процентов атак программ-вымогателей теперь включают компоненты эксфильтрации данных.

Средняя суммарная стоимость атаки программы-вымогателя, включая простой, восстановление и репутационный ущерб, составляет от 1,8 до 5 миллионов долларов за инцидент. Здравоохранение и производство несут наибольшие расходы из-за нарушения операционной деятельности.

Шпионское ПО

Шпионское ПО тайно отслеживает активность пользователя и собирает информацию без его согласия. Оно может отслеживать привычки просмотра веб-страниц, перехватывать нажатия клавиш или собирать персональную информацию.

Характеристики:

- Действует скрытно
- Собирает информацию о пользователе
- Может замедлять работу системы
- Часто поставляется в комплекте с бесплатным ПО
- Трудно обнаружить

Типы:

- **Кейлоггеры**: записывают нажатия клавиш для перехвата паролей
- **Захват экрана**: делают снимки экрана с активностью пользователя

- **Перехватчики браузера**: изменяют настройки браузера, перенаправляют поисковые запросы
- **Отслеживающие файлы cookie**: мониторят поведение при просмотре веб-страниц
- **Коммерческое шпионское ПО**: инструменты типа Pegasus, используемые для наблюдения

Руткиты

Руткит — это вредоносное ПО, предназначенное для обеспечения привилегированного доступа с одновременным сокрытием своего присутствия от средств обнаружения. Название происходит от систем Unix, где "root" — это учётная запись администратора.

Характеристики:

- Скрывается от операционной системы
- Обеспечивает постоянный доступ
- Чрезвычайно трудно обнаружить
- Может модифицировать компоненты ОС
- Для удаления часто требуется полная переустановка системы

Типы:

- **Руткиты пользовательского режима**: работают на уровне приложений
- **Руткиты режима ядра**: работают на уровне ядра ОС
- **Буткиты**: заражают процесс загрузки, загружаются до ОС
- **Руткиты встроенного ПО**: скрываются в прошивке аппаратного обеспечения

Обнаружение руткитов часто требует загрузки с чистого носителя и сканирования системы извне.

Буткиты

Буткит — это продвинутый руткит, который заражает процесс загрузки, загружаясь до операционной системы. Это позволяет ему уклоняться от обнаружения средствами безопасности, которые загружаются после ОС.

Буткиты нацелены на:

- Главную загрузочную запись (MBR)
- Загрузочную запись тома (VBR)
- Прошивку UEFI

Поскольку буткиты загружаются до ОС, они могут перехватывать и изменять любую функцию операционной системы, что делает их чрезвычайно опасными.

Рекламное ПО

Рекламное ПО отображает нежелательную рекламу в системах пользователей. Хотя оно иногда считается менее опасным, чем другие виды вредоносного ПО, рекламное ПО может снижать производительность системы, отслеживать поведение пользователя и служить вектором для более опасного вредоносного ПО.

Характеристики:

- Отображает нежелательную рекламу
- Может отслеживать поведение при просмотре веб-страниц
- Часто поставляется в комплекте с бесплатным ПО
- Может перенаправлять результаты поиска
- Может устанавливать дополнительное нежелательное ПО

Вредоносное ПО для криптоджекинга

Вредоносное ПО для **криптоджекинга** использует системы жертв для майнинга криптовалюты без их согласия. Хотя оно не является деструктивным, оно потребляет вычислительные ресурсы и электроэнергию.

Характеристики:

- Добывает криптовалюту
- Потребляет ресурсы CPU/GPU
- Увеличивает расходы на электроэнергию
- Может вызвать повреждение оборудования из-за чрезмерной нагрузки
- Часто доставляется через браузерные эксплойты

Часть 2: Векторы заражения и распространение

Понимание того, как вредоносное ПО проникает в системы, помогает нам внедрять эффективные средства защиты.

Доставка по электронной почте

Электронная почта остаётся наиболее распространённым механизмом доставки вредоносного ПО:

- **Вредоносные вложения**: документы с макросами, исполняемые файлы
- **Вредоносные ссылки**: ведущие к наборам эксплойтов или загрузкам вредоносного ПО
- **Архивные файлы**: файлы ZIP, RAR, содержащие вредоносное ПО
- **Контрабанда HTML (HTML smuggling)**: кодирование вредоносного ПО в HTML-вложениях

Скрытые загрузки

Пользователи заражаются, просто посещая скомпрометированные веб-сайты:

- Наборы эксплойтов нацелены на уязвимости браузеров
- Не требуется никаких действий пользователя, кроме посещения страницы
- Могут использовать легитимные сайты, которые были скомпрометированы
- Вредоносная реклама доставляет вредоносное ПО через рекламные сети

Уязвимости программного обеспечения

Вредоносное ПО использует уязвимости в программном обеспечении:

- Необновлённые операционные системы
- Устаревшие приложения
- Уязвимости плагинов браузеров
- Эксплойты уязвимостей нулевого дня

Съёмные носители

USB-накопители и другие съёмные носители могут распространять вредоносное ПО:

- Функция автозапуска (в значительной степени отключена в настоящее время)
- Социальная инженерия для запуска вредоносных файлов
- Заражение на уровне встроенного ПО

Распространение по сети

Черви и некоторые другие виды вредоносного ПО распространяются по сетям:

- Эксплуатация уязвимых сервисов
- Использование похищенных учётных данных
- Использование доверительных отношений

Цепочка поставок

Вредоносное ПО может быть внедрено через цепочку поставок программного обеспечения:

- Скомпрометированные обновления ПО
- Заражённые компоненты с открытым исходным кодом
- Троянизированные средства разработки

В 2025 году 29 процентов заражений программами-вымогателями произошли через сторонних поставщиков, по сравнению с 17 процентами в 2024 году.

Часть 3: Углублённый анализ программ-вымогателей

Учитывая распространённость и масштаб последствий программ-вымогателей, рассмотрим их более подробно.

Вымогательство как услуга (RaaS)

Модель RaaS превратила программы-вымогатели в целую криминальную индустрию:

Как работает RaaS:

1. Разработчики создают программы-вымогатели и инфраструктуру
2. Партнёры (аффилиаты) платят за доступ к платформе или арендуют его
3. Партнёры проводят атаки с использованием предоставленных инструментов
4. Прибыль делится (обычно 70-80% достаётся партнёру)

Преимущества для преступников:

- Разработчики получают прибыль, не проводя атаки
- Партнёрам требуется минимум технических навыков
- Масштабируемые криминальные операции
- Общая инфраструктура и поддержка

Эта модель "демократизировала киберпреступность в беспрецедентной степени". Любой человек с базовыми навыками работы в интернете может воспользоваться

этими сервисами.

Двойное и тройное вымогательство

Современные программы-вымогатели выходят за рамки простого шифрования:

Двойное вымогательство:

1. Злоумышленники похищают конфиденциальные данные
2. Злоумышленники шифруют файлы
3. Требуют оплату за расшифровку И предотвращение публикации данных
4. Даже при наличии резервных копий угроза раскрытия данных сохраняется

Тройное вымогательство:

1. Всё вышеперечисленное
2. Плюс DDoS-атаки на жертв
3. Плюс обращение к клиентам или партнёрам жертв
4. Дополнительные методы давления

Более 60 процентов атак программ-вымогателей теперь включают эксфильтрацию данных. Большинство новых группировок, использующих программы-вымогатели, немедленно применяют двойное вымогательство, поскольку это повышает рентабельность инвестиций и снижает переговорные позиции жертвы.

Жизненный цикл атаки программы-вымогателя

Типичное развитие атаки программы-вымогателя:

1. **Первоначальный доступ**: фишинг, уязвимые сервисы, RDP
2. **Закрепление**: установка лазеек (бэкдоров), создание учётных записей
3. **Повышение привилегий**: получение прав администратора
4. **Уклонение от защиты**: отключение средств безопасности
5. **Сбор учётных данных**: похищение паролей
6. **Горизонтальное перемещение**: распространение по сети
7. **Сбор данных**: выявление и похищение ценных данных
8. **Эксфильтрация данных**: извлечение данных на инфраструктуру злоумышленника
9. **Воздействие**: развёртывание программы-вымогателя, шифрование файлов
10. **Вымогательство**: требование оплаты, угроза раскрытия данных

Современные операторы программ-вымогателей часто проводят дни или недели внутри сетей, прежде чем развернуть шифрование.

Новые тактики программ-вымогателей на 2026 год

Формируются новые тенденции:

- **DDoS как услуга**: дополнительное давление на жертв
- **Вербовка инсайдеров**: оплата сотрудникам за предоставление доступа
- **Эксплуатация фрилансеров**: вербовка соучастников в интернете
- **Атаки с использованием ИИ**: автоматизированный выбор жертв и настройка атак
- **Вымогательство с утечкой данных без шифрования**: некоторые группировки полностью отказываются от шифрования

Часть 4: Бесфайловое вредоносное ПО и техника использования штатных средств

Традиционное вредоносное ПО записывает файлы на диск, однако современные злоумышленники всё чаще применяют бесфайловые техники.

Что такое бесфайловое вредоносное ПО?

Бесфайловое вредоносное ПО работает исключительно в оперативной памяти, не записывая постоянных файлов на диск. Это делает его чрезвычайно трудным для обнаружения традиционными антивирусными средствами.

Характеристики:

- Не записывает файлы на диск
- Располагается в оперативной памяти
- Использует легитимные системные инструменты
- Существует только до перезагрузки (если не достигнуто закрепление)
- Уклоняется от обнаружения на основе сигнатур

Число атак бесфайлового вредоносного ПО выросло на 33 процента за последние годы, нацеливаясь на слепые зоны обнаружения на конечных точках.

Техника использования штатных средств (Living-Off-the-Land, L0tL)

Злоумышленники используют легитимные системные инструменты в злонамеренных целях:

Часто используемые злоумышленниками инструменты:

- **PowerShell**: создание скриптов и автоматизация
- **WMI (Windows Management Instrumentation)**: управление системой
- **certutil**: утилита для работы с сертификатами, используемая не по назначению для загрузок
- **bitsadmin**: служба фоновой передачи данных
- **mshta**: выполнение HTA-файлов
- **regsvr32**: регистрация COM-компонентов

Почему техника LOtL эффективна:

- Инструменты уже присутствуют в системах
- Действия могут выглядеть легитимными
- Трудно отличить злонамеренное использование от легитимного
- Невозможно просто заблокировать эти инструменты
- Традиционные антивирусы ориентированы на вредоносные файлы

Проблемы обнаружения

Бесфайловые атаки и атаки с использованием штатных средств требуют иных подходов к обнаружению:

- Поведенческий анализ вместо сигнатур
- Мониторинг командной строки
- Журналирование блоков скриптов
- Анализ памяти
- Аналитика поведения пользователей и сущностей (UEBA)

Часть 5: Основы анализа вредоносного ПО

Специалисты по информационной безопасности анализируют вредоносное ПО для понимания угроз и разработки средств защиты.

Статический анализ

Статический анализ исследует вредоносное ПО без его выполнения:

Методы:

- **Исследование метаданных файла**: заголовки, временные метки, информация о компиляторе
- **Извлечение строк**: поиск URL-адресов, IP-адресов, команд

- **Анализ кода**: дизассемблирование и декомпиляция
- **Вычисление хешей**: генерация индикаторов компрометации для обнаружения
- **Обнаружение упаковщиков**: выявление методов обфускации

Инструменты:

- PEStudio (исполняемые файлы Windows)
- команда strings
- IDA Pro, Ghidra (дизассемблеры)
- VirusTotal (мультисканерный анализ)

Преимущества:

- Безопасный метод (вредоносное ПО не выполняется)
- Может выявить возможности без их активации

Ограничения:

- Обфускация и упаковка усложняют анализ
- Невозможно наблюдать поведение во время выполнения

Динамический анализ

Динамический анализ выполняет вредоносное ПО в контролируемой среде:

Методы:

- **Выполнение в песочнице**: запуск в изолированной виртуальной среде
- **Мониторинг процессов**: наблюдение за созданием и активностью процессов
- **Мониторинг файловой системы**: отслеживание файловых операций
- **Мониторинг реестра**: отслеживание изменений конфигурации
- **Мониторинг сети**: перехват сетевых соединений
- **Мониторинг API**: журналирование системных вызовов

Инструменты:

- Cuckoo Sandbox
- Any.Run (онлайн-песочница)
- Process Monitor
- Wireshark
- API Monitor

Преимущества:

- Раскрывает фактическое поведение

- Позволяет наблюдать распакованный код

Ограничения:

- Вредоносное ПО может обнаружить песочницу и изменить поведение
- Некоторые модели поведения проявляются только при определённых условиях
- Существуют риски при нарушении изоляции

Обход песочницы

Изощрённое вредоносное ПО обнаруживает среды анализа:

Методы обнаружения:

- Проверка на наличие артефактов виртуальных машин (драйверы, ключи реестра)
- Временные атаки (режим ожидания для превышения времени анализа)
- Требование взаимодействия с пользователем
- Проверка среды (имя пользователя, имя машины)
- Снятие отпечатков аппаратного обеспечения

Контрмеры:

- Среды анализа на физическом оборудовании
- Реалистичные конфигурации систем
- Увеличенное время анализа
- Имитация действий пользователя

Часть 6: Защитные технологии

Теперь рассмотрим технологии защиты от вредоносного ПО.

Обнаружение на основе сигнатур

Традиционные антивирусы полагаются на сигнатуры:

- База данных известных шаблонов вредоносного ПО
- Файлы сравниваются с сигнатурами
- Быстрый и точный метод для известных угроз
- Требует регулярного обновления

Ограничения:

- Не может обнаружить новое вредоносное ПО (уязвимости нулевого дня)

- Легко обходится путём модификации
- Неэффективен против бесфайловых атак

Эвристическое обнаружение

Эвристики выявляют вредоносное ПО по паттернам поведения:

- Правила на основе подозрительных характеристик
- Способны обнаруживать варианты известного вредоносного ПО
- Могут выявлять некоторые новые угрозы
- Более высокий уровень ложных срабатываний по сравнению с сигнатурами

Поведенческое обнаружение

Современные решения отслеживают поведение:

- Наблюдение за подозрительными действиями в реальном времени
- Обнаружение вредоносного ПО по его действиям, а не по внешнему виду
- Эффективно против бесфайловых атак и атак с использованием штатных средств
- Может вмешаться до нанесения ущерба

Поведенческие индикаторы:

- Массовое изменение файлов
- Действия по шифрованию
- Внедрение в процессы
- Изменения реестра
- Сетевые аномалии

Обнаружение с помощью машинного обучения

ИИ/МО улучшают обнаружение вредоносного ПО:

- Обучение моделей на характеристиках вредоносного ПО
- Выявление закономерностей, которые может пропустить человек
- Адаптация к новым угрозам
- Снижение зависимости от сигнатур

Ограничения:

- Требуются качественные обучающие данные
- Состязательные атаки способны обходить МО

- Возможны ложные срабатывания
- Проблемы с объяснимостью результатов

Обнаружение и реагирование на конечных точках (EDR)

EDR обеспечивает комплексную защиту конечных точек:

- Непрерывный мониторинг
- Поведенческий анализ
- Возможности проактивного поиска угроз
- Инструменты реагирования на инциденты
- Сбор криминалистических данных

EDR выходит за рамки предотвращения, обеспечивая обнаружение и реагирование на угрозы, которые уклоняются от первоначальных средств защиты.

Изоляция в песочнице

Песочница изолирует потенциально опасный контент:

- Безопасная детонация вложений электронной почты
- Анализ загрузок перед доставкой
- Выполнение подозрительных файлов в изоляции
- Наблюдение за поведением без риска

Часть 7: Практические стратегии защиты от вредоносного ПО

Позвольте поделиться практическими стратегиями защиты от вредоносного ПО.

Эшелонированная защита

Применяйте многоуровневую защиту:

1. Шлюз безопасности электронной почты
2. Веб-фильтрация
3. Защита конечных точек
4. Мониторинг сети
5. Обучение пользователей
6. Резервное копирование и восстановление

Управление обновлениями

Поддерживайте системы в актуальном состоянии:

- Приоритизируйте критические уязвимости
- Тестируйте обновления перед развёртыванием
- По возможности используйте автоматическое обновление
- Отслеживайте статус установки обновлений

Принцип минимальных привилегий

Ограничивайте права пользователей и процессов:

- Пользователи не должны обладать правами администратора для повседневной работы
- Приложения запускаются с минимальными разрешениями
- Снижает последствия успешного заражения вредоносным ПО

Белый список приложений

Разрешайте запуск только одобренных приложений:

- Блокировка выполнения неизвестных программ
- Очень эффективный метод, но требует накладных расходов на управление
- Рекомендуется для сред с высокими требованиями к безопасности

Стратегия резервного копирования

Подготовьтесь к атакам программ-вымогателей:

- Регулярное автоматическое резервное копирование
- Резервные копии на автономных или физически изолированных носителях
- Тестирование процедур восстановления
- По возможности неизменяемые резервные копии
- Правило 3-2-1: 3 копии, 2 типа носителей, 1 внешнее хранилище

Сегментация сети

Ограничивайте распространение вредоносного ПО:

- Изолируйте критически важные системы
- Контролируйте трафик между сегментами

- Отслеживайте попытки горизонтального перемещения

Обучение пользователей

Люди зачастую являются самым слабым звеном:

- Осведомлённость о фишинге
- Правила безопасного поведения в интернете
- Информирование о подозрительной активности
- Регулярное повторное обучение

Заключение

Сегодня мы рассмотрели мир вредоносного программного обеспечения:

1. **Таксономия вредоносного ПО**: вирусы, черви, трояны, программы-вымогатели, шпионское ПО, руткиты и другие
2. **Векторы заражения**: электронная почта, скрытые загрузки, уязвимости, съёмные носители, цепочка поставок
3. **Эволюция программ-вымогателей**: модель RaaS, двойное/тройное вымогательство, новые тактики
4. **Бесфайловое вредоносное ПО**: угрозы, резидентные в памяти, и техники использования штатных средств
5. **Методы анализа**: подходы статического и динамического анализа
6. **Защитные технологии**: сигнатуры, эвристики, поведенческий анализ, МО, EDR, песочницы
7. **Стратегии защиты**: эшелонированный подход, обновления, минимальные привилегии, резервное копирование

На следующей лекции мы рассмотрим социальную инженерию, где злоумышленники нацеливаются на человеческий фактор, а не на технические уязвимости.

Вопросы для обсуждения

1. Должны ли организации платить выкуп? Какие факторы должны влиять на это решение?
2. Как обеспечить баланс между безопасностью и удобством использования при блокировке потенциально вредоносного контента?

3. Какую роль должны играть государства в борьбе с программами-вымогателями?

Благодарю за внимание. До следующей встречи.

Контрольные вопросы

1. Объясните различия между вирусами, червями и троянами. Чем отличаются их методы распространения?
2. Опишите модель "Вымогательство как услуга" (RaaS) и объясните, почему она привела к росту распространённости программ-вымогателей.
3. Что такое двойное вымогательство и как оно меняет оценку рисков для организаций?
4. Опишите бесфайловое вредоносное ПО и технику использования штатных средств. Почему их трудно обнаружить?
5. Сравните статический и динамический анализ вредоносного ПО. В чём сильные стороны и ограничения каждого подхода?
6. Чем современные решения EDR отличаются от традиционных антивирусов на основе сигнатур?
7. Что такое обход песочницы и какие методы используют авторы вредоносного ПО для уклонения от анализа?
8. Опишите стратегию эшелонированной защиты применительно к защите от вредоносного ПО.

Ключевые термины

- **Рекламное ПО (Adware)**: программное обеспечение, отображающее нежелательную рекламу
- **Буткит (Bootkit)**: вредоносное ПО, заражающее процесс загрузки для запуска до операционной системы
- **Криптоджекинг (Cryptojacking)**: несанкционированное использование вычислительных ресурсов для майнинга криптовалюты
- **Двойное вымогательство (Double Extortion)**: тактика программ-вымогателей, объединяющая шифрование данных с их кражей и угрозой публикации похищенных данных в случае неуплаты выкупа
- **Скрытая загрузка (Drive-By Download)**: вредоносное ПО, автоматически загружаемое при посещении скомпрометированного веб-сайта

- **Динамический анализ (Dynamic Analysis)**: процесс анализа поведения вредоносного ПО путём его выполнения в контролируемой среде
- **EDR (Endpoint Detection and Response)**: обнаружение и реагирование на конечных точках — продвинутая система безопасности конечных точек, обеспечивающая видимость и реагирование
- **Бесфайловое вредоносное ПО (Fileless Malware)**: вредоносное ПО, работающее исключительно в памяти без записи файлов на диск
- **Техника использования штатных средств (Living off the Land, LOtL)**: применение легитимных системных инструментов в злонамеренных целях
- **Программа-вымогатель (Ransomware)**: вредоносное ПО, шифрующее данные и требующее оплату за расшифровку
- **Вымогательство как услуга (Ransomware-as-a-Service, RaaS)**: криминальная бизнес-модель, предоставляющая инструменты для создания программ-вымогателей партнёрам
- **Руткит (Rootkit)**: вредоносное ПО, предназначенное для сокрытия своего присутствия и обеспечения постоянного привилегированного доступа
- **Песочница (Sandbox)**: изолированная среда для безопасного анализа подозрительного кода
- **Обход песочницы (Sandbox Evasion)**: методы, используемые вредоносным ПО для обнаружения сред анализа и уклонения от них
- **Шпионское ПО (Spyware)**: программное обеспечение, скрытно собирающее информацию о пользователе
- **Статический анализ (Static Analysis)**: процесс анализа вредоносного ПО без его выполнения, с исследованием структуры кода и сигнатур
- **Троян (Trojan)**: вредоносное ПО, замаскированное под легитимное программное обеспечение
- **Вирус (Virus)**: вредоносное ПО, прикрепляющееся к программам и воспроизводящееся при выполнении программы-носителя
- **Червь (Worm)**: самовоспроизводящееся вредоносное ПО, распространяющееся по сетям без участия пользователя