Пара № 15,16

Отчет

|  |  |  |  |
| --- | --- | --- | --- |
| Образец | Создает файлы | Меняет реестр | Сетевые запросы |
| eicar.com | Нет | Нет | Нет |
| game.exe | Да | Да | Да |

2. Ответы на вопросы

1. Вредоносное поведение может включать создание и изменение файлов, модификацию реестра, выполнение сетевых запросов без ведома пользователя, а также попытки скрыть свое присутствие в системе.

2.EICAR — это тестовый файл, разработанный Европейским институтом компьютерных антивирусных исследований. Он безопасен, так как не содержит вредоносного кода, но позволяет проверить работу антивирусных программ.

3. FakeNet — это инструмент, который симулирует сетевую среду, позволяя аналитикам наблюдать и анализировать сетевые запросы, выполняемые вредоносным ПО, без риска заражения реальной сети.

4. Вредоносное ПО — это любое программное обеспечение, предназначенное для нанесения вреда компьютерной системе. Основные типы включают вирусы, черви, трояны, шпионское ПО, рекламное ПО и программы-вымогатели.

5. Основные цели анализа вредоносного ПО включают понимание его функциональности, методов распространения, способов скрытия и разработку методов защиты и предотвращения атак.

6. Статический анализ включает изучение кода без его выполнения, в то время как динамический анализ подразумевает выполнение кода в контролируемой среде для наблюдения за его поведением.

7. Инструменты для статического анализа включают дизассемблеры (например, IDA Pro), декомпиляторы и анализаторы кода. Они позволяют изучать структуру и логику кода без его выполнения.

8. Обфускация кода — это метод скрытия истинного назначения кода путем его усложнения. Вредоносные программы используют обфускацию, чтобы избежать обнаружения антивирусными программами.

9. Признаки могут включать необычное поведение программы, неожиданные сетевые запросы, изменение системных файлов и реестра, а также попытки скрыть свое присутствие.

10. Песочница — это изолированная среда, в которой можно безопасно выполнять и анализировать вредоносное ПО, не рискуя заразить основную систему.

11. Методы могут включать обфускацию кода, использование полиморфного кода, эксплуатацию уязвимостей и использование социальной инженерии.

12. Инъекция кода — это метод внедрения вредоносного кода в легитимные процессы или программы. Это позволяет вредоносному ПО выполняться в контексте доверенных процессов, избегая обнаружения.

13. Основные этапы включают подготовку среды для анализа, выполнение кода, мониторинг его поведения, сбор и анализ данных о его активности.

14. Статический анализ позволяет извлечь информацию о структуре кода, используемых алгоритмах, строках, функциях и других элементах, которые могут указать на вредоносное поведение.

15. Изучение поведения вредоносных программ позволяет разрабатывать более эффективные методы обнаружения и предотвращения атак, а также улучшать существующие защитные механизмы.

16. Наиболее распространенные сценарии включают кражу данных, шпионаж, выполнение DDoS-атак, распространение спама и вымогательство денег.