Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет безопасности информационных технологий

Дисциплина:

«Основы вирусологии»

ОТЧЕТ ПО КУРСОВОЙ РАБОТЕ

«Анализ вируса-вымогателя WannaCry»

Выполнили:

Бардышев Артём Антонович,

студент группы N3346

(подпись)

Проверил:

,

, ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В мае 2017 года мир столкнулся с одной из самых масштабных и разрушительных кибератак в истории информационной безопасности. Вирус-вымогатель WannaCry (также известный как WannaCrypt, WCry или WanaCrypt0r) поразил сотни тысяч компьютеров в более чем 150 странах мира, нанеся колоссальный экономический ущерб и парализовав работу критически важных инфраструктур, включая больницы, транспортные системы и государственные учреждения.

Уникальность этой атаки заключалась в том, что вирус использовал уязвимость, изначально разработанную Агентством национальной безопасности США (NSA) для собственных целей, которая была украдена и опубликована хакерской группировкой Shadow Brokers. Это событие стало ярким примером того, как инструменты, созданные государственными структурами для киберразведки, могут быть обращены против гражданского населения.

Актуальность темы данной курсовой работы обусловлена тем, что атака WannaCry продемонстрировала новые векторы киберугроз, показала уязвимость современных информационных систем и подчеркнула критическую важность своевременного обновления программного обеспечения. Понимание механизмов работы подобных вредоносных программ необходимо для разработки эффективных мер защиты и предотвращения подобных инцидентов в будущем.

Цель работы – провести комплексный анализ вируса-вымогателя WannaCry, включая историю его возникновения, механизмы распространения и работы, а также оценить последствия атаки и методы защиты.

1 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

1.1 История возникновения и распространения

1.1.1 Предыстория: утечка инструментов NSA

История WannaCry начинается задолго до мая 2017 года. В августе 2016 года хакерская группировка, называющая себя "Shadow Brokers" (Теневые Брокеры), начала публиковать в интернете инструменты и эксплойты, которые, по утверждению группы, были украдены из арсенала Агентства национальной безопасности США (NSA). Среди этих инструментов был эксплойт EternalBlue, который использовал уязвимость в протоколе Server Message Block версии 1 (SMBv1) операционной системы Microsoft Windows.

Уязвимость, получившая идентификатор CVE-2017-0144, позволяла злоумышленникам выполнять произвольный код на удаленных компьютерах без аутентификации, просто отправив специально сформированный пакет данных по протоколу SMB. Microsoft была уведомлена об этой уязвимости и выпустила патч безопасности MS17-010 в марте 2017 года, за два месяца до начала атаки WannaCry. Однако многие организации и частные пользователи не установили это обновление своевременно.

1.1.2 Начало эпидемии

12 мая 2017 года, в пятницу, началась глобальная эпидемия WannaCry. Первые сообщения о заражениях поступили из Великобритании, где вирус поразил компьютеры Национальной службы здравоохранения (NHS). В течение нескольких часов атака распространилась по всему миру, охватив Европу, Азию, Америку и другие регионы.

Вирус распространялся с невероятной скоростью благодаря своей способности к самораспространению. В отличие от традиционных вирусов-вымогателей, которые требуют от пользователя открыть зараженный файл или

перейти по вредоносной ссылке, WannaCry мог самостоятельно находить и заражать уязвимые компьютеры в сети без какого-либо взаимодействия с пользователем.

1.1.3 Хронология событий

12 мая 2017 года:

- 08:00 UTC - массовое распространение по Европе
- 10:00 UTC - атака достигла Азии и Америки
- 15:00 UTC - обнаружен kill switch домен

13 мая 2017 года:

- Британский исследователь Маркус Хатчинс регистрирует kill switch домен
- Распространение вируса значительно замедляется
- Microsoft выпускает экстренные патчи для устаревших версий Windows

14-15 мая 2017 года:

- Появляются новые варианты вируса с измененными kill switch доменами
- Исследователи продолжают регистрировать новые домены для блокировки распространения

1.2 Масштабы эпидемии

1.2.1 Географическое распространение

По оценкам экспертов, WannaCry заразил более 300 000 компьютеров в 150 странах мира. Наибольшее количество заражений было зафиксировано в следующих странах:

- Россия - более 1000 организаций, включая МВД, Следственный комитет, Минздрав

- Украина - массовые заражения в государственных учреждениях и банках

- Индия - тысячи зараженных компьютеров

- Тайвань - компания TSMC была вынуждена приостановить производство

- Великобритания - серьезно пострадала Национальная служба здравоохранения

- Испания - заражены компьютеры телекоммуникационной компании Telefónica

- Германия - пострадали Deutsche Bahn и другие организации

1.2.2 Динамика распространения

Согласно данным различных аналитических центров:

- Пиковая скорость распространения: до 10,000 заражений в час

- Количество выплаченных выкупов: около $130,000 (по данным отслеживания биткойн-кошельков)

- Экономический ущерб: от $4 до $8 миллиардов долларов

В первые 24 часа атаки вирус распространялся экспоненциально. Каждый зараженный компьютер начинал сканировать сеть на наличие других уязвимых машин, создавая эффект "снежного кома". Без вмешательства исследователей, обнаруживших kill switch, количество заражений могло бы достичь миллионов.

1.3 Авторство и происхождение вируса

1.3.1 Первоначальные версии

Сразу после начала атаки эксперты по кибербезопасности начали расследование с целью установления авторства вируса. Первоначально подозрения пали на Северную Корею, так как код WannaCry имел определенное

сходство с предыдущими атаками, приписываемыми хакерской группе Lazarus, которая, по мнению экспертов, действует в интересах КНДР.

1.3.2 Лингвистический анализ

Специалисты по кибербезопасности из компании Flashpoint провели детальный лингвистический анализ текстов сообщений с требованием выкупа, которые отображались на экранах зараженных компьютеров. Анализ показал, что оригинальный текст был написан на китайском языке, причем с использованием южного диалекта, характерного для провинций Гуандун, Фуцзянь или близлежащих регионов.

Исследователи обнаружили специфические языковые конструкции и термины, которые указывали на то, что авторы вируса были носителями южного диалекта китайского языка. Это привело к предположениям, что создатели WannaCry могут быть выходцами из: Южных регионов Китая, Гонконга, Тайваня, Сингапура.

1.3.3 Технические индикаторы

Анализ кода WannaCry выявил несколько технических индикаторов, которые могли указывать на авторство:

- Использование техник, характерных для группы Lazarus
- Сходство с предыдущими атаками на финансовые учреждения
- Использование инструментов, ранее применявшихся в атаках, приписываемых КНДР

Однако эти индикаторы не являются окончательным доказательством, так как могут быть результатом копирования техник или намеренной дезинформации.

1.4 Социальные и политические последствия

Атака WannaCry имела не только экономические, но и серьезные социальные и политические последствия:

- Повысилась осведомленность общественности о киберугрозах
- Правительства различных стран пересмотрели свои стратегии кибербезопасности
- Усилилось международное сотрудничество в области борьбы с киберпреступностью
- Поднялись вопросы о безопасности инструментов, разрабатываемых государственными структурами

2 ПРАКТИЧЕСКАЯ ЧАСТЬ

2.1 Архитектура вируса

2.1.1 Общая структура

WannaCry представляет собой сложный многоуровневый вредоносный комплекс, состоящий из нескольких взаимосвязанных компонентов. Архитектура вируса включает следующие основные модули:

1. Dropper (Загрузчик) - основной исполняемый файл, который инициирует процесс заражения

2. Network Scanner (Сетевой сканер) - модуль для поиска уязвимых компьютеров в сети

3. Exploit Module (Модуль эксплойта) - компонент, использующий уязвимость EternalBlue

4. Encryption Module (Модуль шифрования) - компонент для шифрования файлов

5. Ransomware Module (Модуль вымогателя) - компонент, отображающий сообщения с требованием выкупа

6. Task Scheduler Module (Модуль планировщика задач) - компонент для обеспечения персистентности

2.1.2 Компоненты вируса

Основной исполняемый файл (Dropper):

Dropper является точкой входа вируса в систему. Этот компонент выполняет следующие функции:

- Проверка наличия kill switch домена

- Распаковка и запуск основных модулей вируса

- Создание задач в планировщике Windows для обеспечения автозапуска

- Удаление теневых копий файлов (Volume Shadow Copies) для предотвращения восстановления

Сетевой модуль:

Сетевой модуль отвечает за распространение вируса по сети. Он включает:

- Сканер портов для поиска открытых SMB-портов (445/TCP)

- Генератор случайных IP-адресов для сканирования

- Модуль для использования уязвимости EternalBlue

- Бэкдор DoublePulsar для загрузки и выполнения кода на удаленных машинах

Модуль шифрования:

Модуль шифрования является сердцем вируса-вымогателя. Он выполняет:

- Поиск файлов для шифрования по определенным расширениям

- Генерацию криптографических ключей

- Шифрование файлов с использованием гибридной схемы (RSA + AES)

- Переименование зашифрованных файлов с добавлением расширения ".WNCRY"

2.1.3 Взаимодействие компонентов

Все компоненты вируса тесно интегрированы и работают в определенной последовательности:

1. Dropper проверяет kill switch и распаковывает модули

2. Network Scanner начинает поиск уязвимых машин

3. Exploit Module использует EternalBlue для заражения найденных машин

4. Encryption Module шифрует файлы на зараженной машине

5. Ransomware Module отображает сообщение с требованием выкупа

2.2 Механизм распространения

2.2.1 Уязвимость EternalBlue

Основой механизма распространения WannaCry является уязвимость EternalBlue (CVE-2017-0144) в протоколе SMBv1. Эта уязвимость представляет собой переполнение буфера в функции обработки SMB-запросов, которая позволяет злоумышленнику выполнить произвольный код на удаленной машине.

Технические детали уязвимости:

- Протокол: SMBv1 (Server Message Block version 1)

- Порт: 445/TCP

- Тип уязвимости: Remote Code Execution (RCE)

- Требования: Отсутствие аутентификации не требуется

- Затронутые версии Windows: Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008, Windows 8, Windows Server 2012, Windows 10 (до версии с патчем MS17-010)

Механизм эксплуатации:

1. Злоумышленник отправляет специально сформированный SMB-пакет на уязвимую машину

2. Из-за ошибки в обработке пакета происходит переполнение буфера

3. Переполнение позволяет перезаписать адрес возврата функции

4. Выполняется shellcode, загруженный злоумышленником

5. Shellcode устанавливает бэкдор DoublePulsar

2.2.2 Алгоритм самораспространения

WannaCry использует сложный алгоритм для поиска и заражения уязвимых машин:

Этап 1: Генерация IP-адресов

Вирус генерирует случайные IP-адреса для сканирования. Алгоритм генерации включает:

- Случайные IP-адреса в диапазоне 0.0.0.0 - 255.255.255.255

- Приоритет локальной сети (сканирование локальных адресов)

- Избегание определенных диапазонов (например, адресов IANA)

Этап 2: Сканирование портов

Для каждого сгенерированного IP-адреса вирус:

- Проверяет доступность порта 445/TCP

- Определяет, работает ли на порту служба SMB

- Проверяет версию протокола SMB

Этап 3: Эксплуатация уязвимости

Если найдена уязвимая машина:

- Отправляется эксплойт EternalBlue

- Устанавливается бэкдор DoublePulsar

- Загружается и выполняется модуль WannaCry

Этап 4: Репликация

Зараженная машина сама становится источником заражения и начинает сканировать сеть, создавая эффект "снежного кома".

2.3 Процесс заражения

2.3.1 Инициализация

Процесс заражения начинается с запуска основного исполняемого файла (dropper). При запуске вирус выполняет следующие действия:

1. Проверка окружения:
   - Определение версии операционной системы
   - Проверка наличия административных прав
   - Проверка наличия антивирусного ПО
2. Проверка kill switch:
   - Попытка подключения к домену `www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com`

- Если домен доступен - вирус прекращает работу

- Если домен недоступен - продолжается процесс заражения

3. Распаковка модулей:

- Извлечение зашифрованных модулей из ресурсов исполняемого файла

- Расшифровка модулей в памяти

- Загрузка модулей в память процесса

2.3.2 Установка в систему

После инициализации вирус устанавливается в систему для обеспечения персистентности:

1. Создание файлов:

- Копирование основного модуля в директорию `%ProgramData%` или `%AppData%`

- Создание файла `tasksche.exe` (основной модуль)

- Создание файла `@WannaDecryptor@.exe` (модуль вымогателя)

2. Создание задач в планировщике:

- Создание задачи с именем, содержащим случайные символы

- Настройка автозапуска при загрузке системы

- Настройка периодического запуска

3. Модификация реестра:

- Добавление записей в автозагрузку (в некоторых версиях)

- Изменение настроек безопасности

2.3.3 Удаление защитных механизмов

Перед началом шифрования вирус пытается отключить защитные механизмы Windows:

1. Удаление теневых копий:

```
vssadmin delete shadows /all /quiet
wmic shadowcopy delete
```

2. Остановка служб:

- Остановка службы Volume Shadow Copy
- Остановка службы Windows Backup
- Остановка службы Windows Defender (если возможно)

3. Блокировка доступа:
- Блокировка доступа к диспетчеру задач
- Блокировка доступа к редактору реестра
- Блокировка доступа к командной строке

2.3.4 Начало шифрования

После завершения подготовки вирус начинает процесс шифрования файлов:

1. Поиск файлов:
- Рекурсивный обход всех дисков и директорий
- Фильтрация файлов по расширениям
- Исключение системных файлов и файлов вируса

2. Генерация ключей:
- Генерация уникального AES-ключа для каждого файла
- Шифрование AES-ключа с помощью RSA-публичного ключа
- Сохранение зашифрованного ключа вместе с файлом

3. Шифрование:
- Чтение файла по частям
- Шифрование каждой части с помощью AES
- Запись зашифрованных данных обратно в файл
- Переименование файла с добавлением расширения ".WNCRY"

2.3.5 Типы шифруемых файлов

WannaCry шифрует файлы со следующими расширениями:

Документы (.doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .rtf, .txt, .odt, .ods, .odp)

Изображения (.jpg, .jpeg, .png, .gif, .bmp, .psd, .ai, .svg)

Архивы (.zip, .rar, .7z, .tar, .gz)

Базы данных (.mdb, .sql, .db)

Разные (.mp3, .mp4, .avi, .mkv, .cpp, .java, .py)

- И многое другое (более 170 расширений)

2.3.5 Исключения

Вирус не шифрует файлы в следующих директориях:

- `%ProgramData%\Microsoft\Windows\Start Menu\Programs\Startup`
- `%AppData%\Microsoft\Windows\Start Menu\Programs\Startup`
- Системные директории Windows
- Директории с файлами вируса

Также не шифруются файлы с расширениями:

- .exe, .dll, .sys (системные файлы)
- .WNCRY (уже зашифрованные файлы)
- Файлы меньше определенного размера (в некоторых версиях)

ЗАКЛЮЧЕНИЕ

Атака вируса-вымогателя WannaCry в мае 2017 года стала одним из самых значимых событий в истории кибербезопасности. Эта эпидемия продемонстрировала несколько критически важных моментов:

Во-первых, WannaCry показал, насколько уязвимыми могут быть современные информационные системы, даже когда патчи для известных уязвимостей уже доступны. Многие организации пострадали не из-за отсутствия защиты, а из-за несвоевременного применения обновлений безопасности.

Во-вторых, атака продемонстрировала опасность использования инструментов, разработанных государственными структурами для киберразведки. Утечка эксплойта EternalBlue из арсенала NSA и его использование злоумышленниками показала, что такие инструменты могут быть обращены против гражданского населения.

В-третьих, WannaCry подчеркнул важность резервного копирования данных. Организации, которые регулярно создавали резервные копии, смогли быстро восстановиться после атаки, в то время как те, кто пренебрегал этой практикой, понесли значительные потери.

В-четвертых, атака показала важность международного сотрудничества в области кибербезопасности. Обнаружение kill switch британским исследователем и быстрое реагирование сообщества кибербезопасности помогло предотвратить еще больший ущерб.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Kaspersky Lab. (2017). *WannaCry: история интернет-червя*. Блог Касперского. URL: https://www.kaspersky.ru/blog/wannacry-hsitory-lessons/33853/

2. Securelist. (2017). *WannaCry ransomware: Technical analysis*. Kaspersky Lab. URL: https://securelist.com/wannacry-ransomware-technical-analysis/78431/

3. Symantec Security Response. (2017). *WannaCry: Ransomware attacks show strong links to Lazarus group*. Symantec Official Blog. URL: https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attacks-show-strong-links-lazarus-group

4. Microsoft Security Response Center. (2017). *Customer Guidance for WannaCrypt attacks*. Microsoft TechNet. URL: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

5. InfoWatch. (2017). *Справка Аналитического центра InfoWatch об атаке вируса WannaCry*. InfoWatch Analytics. URL: https://www.infowatch.ru/analytics/utechki-informatsii/spravka-analiticheskogo-tsentra-infowatch-ob-atake-virusa-wannacry

6. Habr. (2017). *WannaCry: анализ, индикаторы компрометации и рекомендации по предотвращению*. Хабр. URL: https://habr.com/ru/companies/cisco/articles/328598/