МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Разработка маскирующего файлового шредера

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Скундина Константина Михайловича

Научный руководитель
к.ю.н., доцент _____ А. В. Гортинский
22.01.2022 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
22.01.2022 г.

Саратов 2022

ВВЕДЕНИЕ

Успешное затирание файла на диске состоит из 3-х этапов: удаление указателя на файл, затирание пространства на диске, где размещался файл и удаление всей информации, указывающей на существование удаляемого файла.

Удаление файла в большинстве операционных систем просто удаляет указатель на файл без затирания его содержимого, поскольку время затирания файла занимает примерно столько же времени сколько и его запись на диск. После такого удаления файл легко обнаруживается многими приложениями восстановления. Однако, как только на пространство диска, где размещался файл, записываются другие данные, нет никакого гарантированного способа восстановить удаленную информацию. Ни одна частная компания по восстановлению информации не берётся утверждать, что способна восстановить полностью перезаписанные данные.

Как правило, уничтожение данных используются государственными учреждениями, прочими специализированными структурами и предприятиями в целях сохранения государственной или коммерческой тайны. Уничтожение данных используется также в средствах программного шифрования информации для безопасного удаления временных файлов и уничтожения исходных. Также важным пунктом является сокрытие самого факта перезаписи, поскольку в противном случае, если злоумышленник обнаружит следы существования, интересующего его файла, он продолжит исследовать носитель на наличие других файлов, связанных с нужным. Таким образом существует возможность полного или частичного восстановления исходного файла лицом, желающим получить доступ к личной или секретной информации.

Целью дипломной работы является:

- Исследование файловой системы NTFS;
- Исследование следообразования в ОС Windows;

- Создание программы, способной уничтожать как сведения об указанном файле, так и все служебные записи и временные данные, возникающие в процессе обработки файлов;
- Маскировка факта удаления и использования программы.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 1 приложения. Общий объём работы – 58 страниц, из них 32 страницы – основное содержание, включая 23 рисунка и 4 таблицы, список использованных источников из 8 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В разделе 1 «Структура системных областей файловой системы NTFS» приводятся основные теоретические понятия, необходимые для дальнейшего рассмотрения темы. Приводится основная структура файловой системы NTFS, позволяющая раскрыть её архитектуру, а также основные атрибуты.

Современной файловой системой, используемой в операционной системе Windows, является NTFS – New Technology File System. Каждый раздел файловой системы NTFS организован в виде последовательности блоков, называемых кластерами. Большинство дисков NTFS использует кластеры размером 4 Кбайта. При формировании файловой системы NTFS создаётся файл MFT – Master File Table, а также создаются другие области для хранения метаданных файла. Метаданные используются NTFS для реализации файловой структуры. К ним относятся данные, описывающие файлы или каталоги. Все метаданные хранятся в атрибутах. Основные рассмотренные атрибуты:

- $STANDART_INFORMATION;
- $FILE_NAME;
- $DATA.

В разделе 2 «Процессы следообразования» приводятся основные системные области для изучения следообразования в ОС Windows.

В подразделе 2.1 «Особенности хранения файла» приводится информация об особенностях хранения файла в ОС Windows.

Файловая система считается областью данных, и любой сектор диска может быть выделен файлу. Однако должно соблюдаться условие, что первые сектора тома содержат загрузочный сектор и загрузочный код.

Сам файл и информация об этом файле сохраняется в различных местах. Даже если файл был затерт, то всё ещё можно найти факт его существования на жёстком диске.

Пользователь может удалить сам файл, и если файл становится негодным для восстановления, то его данные могут быть найдены в других файлах, которые сам пользователь не создавал. Данные могут быть невидимы через стандартный интерфейс, но могут быть обнаружены в нескольких местах, таких как остаточное пространство и нераспределенное пространство. Остаточное пространство – это пространство между концом файла и концом кластера.

В подразделе 2.2 «Следообразование в каталогах ОС Windows» указаны основные каталоги ОС Windows, важные для исследования следообразования, а впоследствии для ликвидации найденных следов удаления и использования программ для затирания.

Файл подкачки (pagefile.sys) – файл свопинга, хранящий дамп оперативной памяти, хранится в корневом каталоге диска. В нем находятся выгрузки областей задач и буферные зоны, не помещающиеся в физическом ОЗУ.

Каталог «System Volume Information». Хранится также в корневом каталоге. В случае если служба восстановления системы с помощью точек отката активна, то хранит информацию о содержимом ветвей реестра и иных системных файлов до внесения изменений инсталляторами или при создании такой точки по желанию пользователя.

Домашний каталог пользователя. В этом каталоге хранятся индивидуальные настройки пользователя и журналы, создаваемые различными программами, в том числе файлы историй и т.д. В каталоге Recent содержатся ярлыки тех файлов, что недавно использовались.

Каталог «%Системный диск%\Windows\INF» может хранить inf-файлы устанавливаемых таким образом приложений или драйверов.

Каталог «%Системный диск%\Windows\Prefetch» хранит pf-файлы, которые содержат информацию об обстоятельствах запуска приложений в данном экземпляре ОС.

Каталог «%Системный диск%\system32\config» содержит файлы системных журналов: системы, безопасности, приложений, а также файлы системного реестра.

В подразделе 2.3 «Следообразование в системном реестре ОС Windows» рассмотрена структура системного реестра. Представлена информация о временных метках, хранящихся в ключах реестра, а также информация о процессе удаления информации, хранимой в ячейках.

Реестр в ОС Windows является базой, хранящей все её основные настройки. В том числе и настройки, касающиеся расположения и наличия некоторых других областей следообразования. Физически Windows организует реестр в виде кустов или ульев, хранящихся в двоичных файлах. Кроме того, для каждого улья, ОС создает дополнительные файлы, которые содержат резервные копии улья.

Все ключи реестра содержат временную метку, похожую на дату последнего изменения для файлов. Это значение хранится в структуре FILETIME. При попытке сокрытия следов какого-либо события, злоумышленники могут изменять данные в записях, отвечающих за хранение времени последнего изменения. В этом случае значение временной метки позволяет не только установить истинное время какого-либо события, но и установить факты намеренного редактирования реестра с целью сокрытия следов.

Большинство информации, хранимой в ячейках, сохраняется при их удалении; однако, некоторые ключевые данные уничтожаются, причем правила удаления для различных типов ячеек различаются. При удалении подключа его индекс удаляется из списка подключей родителя, и список перезаписывается в соответствующую ячейку. Значение удаляется аналогично.

Информация о подключавшихся USB-устройствах хранится в ветке HKLM\System\ControlSet00x\ENUM\USBSTOR. В этой ветке реестра создаются ключи, каждый из которых представляет свой класс устройств.

В разделе 3 «Интерфейс реализованной программы» представлена реализованная в ходе дипломной работы программа, способная затирать выбранные файлы на диске.

В подразделе 3.1 «Возможности программы» продемонстрированы реализованные функции программы:

- Показать информацию о файле/каталоге;
- Поиск дубликатов файла;
- Поиск всех дублирующихся файлов в каталоге;
- Поиск удалённых записей в MFT таблице;
- Поиск связанной информации в каталогах Windows по найденным ранее именам файлов;
- Поиск недавно использованных программ в каталоге Prefetch;
- Поиск и удаление связанной информации в системном реестре Windows по найденным ранее именам файлов;
- Полное затирание на диске файла и всей найденной ранее информации. В случае каталога применяется ко всем вложенным файлам и каталогам.

В подразделе 3.2 «Процедура затирания файловой записи» рассмотрена особенность использования файловой системы для настройки правильного доступа к диску и возможности прямой записи на него.

Во время затирания любой файловой записи используется контрольный код «FSCTL_DISMOUNT_VOLUME» для размонтирования тома. Этот код отключает том независимо от того, используют ли этот том какие-либо другие процессы, что может иметь непредсказуемые результаты для этих процессов, если они не удерживают блокировку тома. Операционная система пытается смонтировать отключенный том, как только будет предпринята попытка получить к нему доступ. Для избегания подобных случаев используется второй контрольный код «FSCTL_LOCK_VOLUME». При использовании данного кода получить доступ к тому может только тот процесс, что использовал данный код.

В подразделе 3.3 «Процедура затирания файла» рассмотрен используемый в программе алгоритм для затирания файла, а также представлен наглядный пример использования данного алгоритма.

Процедура перезаписи кластеров файла выглядит следующим образом. Программа получает информацию о всех фрагментах файла и информацию о MFT-записи файла. Далее идёт покластерная перезапись дискового пространства, выделенного под файл. С помощью winapi-функции *ReadFile* программа считывает первый найденный кластер диска, не принадлежащий файлу и с помощью winapi-функции *WriteFile* записывает его на место первого кластера файла. Считывается следующий найденный кластер диска, не принадлежащий файлу и записывается вместо второго кластера файла и т.д..

В подразделе 3.4 «Процедура удаления ключа реестра» рассмотрен используемый в программе алгоритм для поиска и удаления ключей реестра, а также представлен наглядный пример использования данного алгоритма.

С помощью функций реестра для Win32 проводится поиск ключей, подстрокой которых являются имена из ранее сформированного списка – списка найденных имён файлов.

В разделе 4 «Сравнение с аналогами» рассмотрены наиболее популярные аналоги реализованной программы.

В подразделе 4.1 «CCleaner» представлена информация о соответствующем программном обеспечении.

По сравнению с реализованной программой недостатком такого инструмента является то, что нельзя выбрать конкретный файл или несколько файлов для выборочного затирания, а преимуществом является выбор критерия поиска и фильтрация файлов.

В подразделе 4.2 «Active KillDisk» представлена информация о соответствующем программном обеспечении.

По сравнению с реализованной программой преимуществом программы является способность обнаруживать разделы, называемые «Unallocated Space». Это нераспределённая область диска, в которой отсутствует раздел или том.

В подразделе 4.3 «File Shredder» представлена информация о соответствующем программном обеспечении.

По сравнению с реализованной программой достоинством программы является интеграция функции удаления в контекстное меню проводника Windows, что позволяет использовать алгоритмы программы для удаления файла прямо из каталога.

В подразделе 4.4 «Freeraser» представлена информация о соответствующем программном обеспечении.

По сравнению с реализованной программой следы удаления от использования данной программы могут быть найдены в нераспределённой области диска. Также информация об удалённых файлах может быть обнаружена в файле подкачки.

ЗАКЛЮЧЕНИЕ

В ходе дипломной работы были разобраны структура файловой системы NTFS, была изучена документация Microsoft, связанная с программированием на низшем уровне, были изучены процессы следообразования ОС Windows в каталогах и реестре.

Была реализована программа, предназначением которой является дефрагментация файла и ликвидация всей связанной с этим файлом информацией с применением сокрытия данных процедур удаления. Для сокрытия факта удаления применялись различные методы, такие как поиск связанных с файлом данных, поиск дубликатов файлов и последующая их перезапись кластерами-соседями, поиск по MFT-таблице, поиск в домашнем каталоге пользователя.

Также в работе была раскрыта важность того, что перезаписать данные не всегда бывает достаточно, необходимо ещё и скрыть факт этой самой перезаписи. Это важно потому, что файл и различные связанные с ним данные могут быть разбросаны по разным секторам диска, и в случае если злоумышленник обнаружит факт перезаписи секретного файла, то у него будет весомый повод начать поиск какой-либо информации, указывающей на то, что было в этих секторах.

Задачи реализованы в полной мере для несистемного раздела NTFS. Реализованная программа может применяться как альтернатива существующим файловым шредерам.