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

Получение связанной информации об аппаратном обеспечении и сетевых подключениях в ОС Windows и определение временных рамок

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Якушева Святослава Александровича

Научный руководитель
доцент _____ А. В. Гортинский
21.01.2023 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
21.01.2023 г.

Саратов 2023

ВВЕДЕНИЕ

Цифровизация человеческой деятельности, экспоненциально растущая с начала 21 века, неизбежно повышает интерес учёных к различным аспектам исследования компьютерных систем с целью получения криминалистически значимой информации. В информационной среде, которая образуется в результате работы компьютерных устройств и их взаимодействия посредством телекоммуникационных каналов связи, отражаются, фиксируются и сохраняются специфические следы различной человеческой деятельности, в том числе, преступной.

В данной работе предметом исследования будет реестр операционной системы Windows. Среди компьютерных операционных систем Windows остается безусловным лидером. По статистическим данным, на 2021 год Windows занимает лидирующую позицию с 75,4% пользователей. Этот факт подчеркивает важность изучения реестра Windows, так как большинство инцидентов с участием компьютерных устройств могут быть расследованы на основе информации в нем.

От компании Microsoft опубликовано мало информации, связанной со спецификой того, как информация реестра организована в структуры данных на диске. Однако, различные разработчики программных продуктов с открытым исходным кодом работают над этим и опубликовывают технические детали, необходимые для написания программного обеспечения, совместимого с форматом реестра Microsoft. Однако эти источники в целом неполны и фрагментированы, что затрудняет разработку инструментов.

Существуют также программные продукты, способные получать информацию из файлов пассивного реестра, однако о тех, что способны выводить связанную информацию информации не нашлось.

По ходу работы мы соберем всю доступную информацию о строении файлов пассивного реестра и получения из них информации, и о том, как полученные данные связывать. На основе полученных знаний реализуем

программу, способную выводить связанную информацию из файлов пассивного реестра Windows.

Дипломная работа состоит из введения, трех основных разделов, которые, в свою очередь, содержат подразделы, заключения, списка использованных источников и двух приложений. Общий объем работы – 108 страниц, из них 39 страниц – основное содержание, включая 27 рисунков и 9 таблиц, список использованных источников из 18 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

1 Глава 1. Реестр Windows. Описание строения

Первый раздел данной дипломной работы имеет название «Реестр Windows. Описание строения». В нем описывается устройство файлов пассивного реестра. Данная информация необходима для получения данных из этих файлов.

Глава содержит девять подразделов. Подраздел 1.1 называется «Обзор структуры». В нем рассматривается внутренняя структура данных в реестре.

Реестр Windows реализован в виде древовидной структуры и аналогичен файловой системе. Например, значения реестра схожи с файлами в файловой системе поскольку они хранят имя и тип информации для дискретных частей необработанных данных. Ключи реестра очень похожи на каталоги файловой системы, выступая в качестве родительских узлов как для подразделов, так и для значений.

Внутренняя структура кустов реестра Windows, однако, сильно отличается от типичных файловых систем. Основное отличие состоит в том, что ключи ссылаются на значения иначе, чем подразделы, в то время как большинство файловых систем ссылаются и на значения, и на подразделы, используя одни и те же структуры. Кроме того, из-за типа хранения (двоичный файл), выделение памяти для структур данных осуществляется таким образом, чтобы свести к минимуму фрагментацию и линейное использование пространства.

Подраздел 1.2 «Файлы реестра» содержит обзор стандартных файлов реестра и структуру их заголовков.

В разделе 1.3 «Контейнеры куста (Hive Bins)» говорится о такой структуре внутри файлов реестра как контейнеры куста.

Файлы куста реестра размещаются в блоках по 4096 байт, начиная с заголовка, или базового блока, после которых следуют серии блоков данных куста. Размер каждого контейнера куста (HBIN) обычно составляет 4096 байт, но может быть и больше, кратным этому размеру. HBIN связаны друг с другом.

Внутри каждого HBIN можно найти ряд ячеек переменной длины. Значения ячеек улья содержат различные типы данных.

Далее в этом же подразделе рассматривается структура заголовка контейнера куста, сигнатуры типов данных.

Раздел 1.4 «Ключи» описывает множество таких структур данных как ключевые записи. Структура данных, которая связывает все элементы вместе, является ключевой записью (NK). Записи NK содержат ряд полей смещения к другим структурам данных. Эти упомянутые структуры могут существовать в любом HBIN. А также записи NK содержат поля времени модификации (MTIME).

Для следует подраздел 1.5 «Списки подразделов и значений». Списки подразделов – это простые списки указателей/хеш-кортежей, отсортированные по хэш-значению, которое основано на именах подключа, на которые ссылаются. Списки значений похожи на списки подразделов, но не имеют связанных с ними хеш-значений и не сортируются в каком-либо определенном порядке. Записи VK содержат минимум метаданных об единственном значении и хранят смещение другой ячейки, хранящей данные значения.

Подраздел 1.6 содержит информацию о ключах безопасности. В кустах реестра хранится небольшое количество записей безопасности (SK – security key). На них ссылаются записи NK. Записи SK включают короткий заголовок, за которым следует дескриптор безопасности Windows, определяющий разрешения и владельца для локальных значений и/или подразделов.

В 1.7 показывается как связываются между собой рассмотренные ранее структуры данных.

В подглаве 1.8 говорится о хранилищах данных значений. В большинстве случаев данные значений хранятся просто в ячейке без какой-либо реальной структуры, кроме той, которая определяется типом данных. Однако, если значение имеет длину четыре или меньше байта, Windows может предпочесть сохранить данные в поле смещения записи VK (value key). Кроме того, начиная с Windows XP, записи значений данных могут быть фрагментированы на

несколько ячеек с использованием записей «больших данных». Также здесь рассматривается структура записей VK.

Наконец в подразделе 1.9 рассматриваются типы данных значений. Значения реестра могут быть одного из нескольких различных типов. Тип данных значения хранится в виде 32-битного целого числа в записи VK, и на основе этого типа данных ячейка данных должна соответствовать определенному формату.

2 Глава 2. Следообразование в реестре Windows

В данной главе содержатся 11 подразделов. В ней рассматривается следообразование в реестре Windows, описываются основные виды следов и способы их обнаружения.

Раздел 2.1 содержит информацию о видах связывания информации в реестре Windows. Зачастую, информация в реестре не содержится вся в конкретном ключе. Для получения полных данных информацию из множества ключей необходимо связать. Критерием для связи может быть имя ключа или дополнительная информация, хранимая в нем.

В разделе 2.2 описывается определение конфигурации системы. Во время вскрытия системного реестра нам может понадобиться определить, какой ControlSet был загружен как CurrentControlSet, когда система работала. Для этого все, что нам нужно сделать, это просмотреть значения в ключе Select в кусте System. В ключе Select значение Current сообщает нам, какой ControlSet был загружен как CurrentControlSet при работе системы.

Подраздел 2.3 Содержит информацию о том, в каких ключах реестра можно найти следы подключения USB-устройств и как эти следы образуются. Когда USB-устройство подключено к системе Windows, диспетчер Plug-and-Play (PnP) получает уведомление и запрашивает устройство. Информация об устройстве, извлеченная из дескриптора устройства (не являющегося частью области памяти устройства), затем сохраняется в кусте System в подразделах CurrentControlSet\Enum\USBStor и \USB. Затем запоминающее устройство

(чаще всего) распознается как дисковое устройство и монтируется в системе как буква диска/том. Таким образом, дополнительная информация, относящаяся к устройству, записывается в ключе MountedDevices в кусте System, а также в двух подразделах под ключом Control\DeviceClasses.

В подразделе 2.3.1 говорится о там, как получить точное время последнего подключения USB-устройства. Для получения времени последнего подключения USB-устройства следует взять временную метку одного из подключей ключа SYSTEM\ControlSet00x \Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Глава 2.4 «Сопоставление устройств с буквами дисков». Здесь рассказывается как работать с данными в ключе MountedDevices, и как с их помощью связать устройства с буквами дисков.

Раздел 2.5 «Сопоставление букв диска с жесткими дисками» является продолжением предыдущего раздела.

Подраздел 2.6 ведется рассказ о классах устройств. Когда USB-устройство впервые подключается к системе Windows, диспетчер PnP запрашивает устройство, чтобы определить информацию об устройстве, выяснить, какие драйверы для этого устройства необходимо загрузить. После загрузки устройства для него создаются два дополнительных ключа под ключом DeviceClasses в кусте System. Оба этих ключа глобально уникальные идентификаторы (GUID); один относится к дискам, а другой к томам.

Раздел 2.7 содержит список ключей, в которых содержится информация о принтерах.

«Сетевые интерфейсы» – раздел 2.8. Подобно другим устройствам, информация о сетевых интерфейсах, доступных в системе, хранится в кусте System. Основной путь для получения информации о сетевых интерфейсах – ключ ControlSet00n\Services\Tcpip\Parameters\Interfaces. Под этим ключом вы найдете несколько подразделов, имена которых являются глобальными уникальными идентификаторами – GUID. Каждый из этих подразделов

относится к определенному интерфейсу, а GUID имена могут быть преобразованы в более просто читаемые имена интерфейсов.

2.9 «Сетевые карты». Информация о сетевых адаптерах также хранится в кусте Software. Под путем к ключу Microsoft\Windows NT\CurrentVersion\NetworkCards вы можете увидеть несколько пронумерованных подразделов. Каждый из этих подразделов относится к интерфейсу.

Глава 2.10 содержит информацию о беспроводных соединениях. Информация о беспроводных соединениях, а именно подключениях к точкам беспроводного доступа (WAP), хранится в подразделах GUID под ключом Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles в кусте Software. В этих ключах содержится такие значения как дата создания профиля (первое подключение системы к) и время последнего подключения системы к WAP (рисунок 23). Данные в этих значениях, а именно DateCreated и DateLastConnected соответственно, немного больше, чем мы ожидаем для объектов времени Unix (32-разрядных) или FILETIME (64-разрядных). Данные внутри этих значений на самом деле являются 128-битными объектами SYSTEMTIME. Это важно, поскольку это еще один формат меток времени, к которому мы должны быть готовы при анализе систем Windows.

3 Глава 3. Практическая часть

Третий раздел является описанием того, что было реализовано в ходе данной дипломной работы. В ходе дипломной работы была реализована программа в виде консольного приложения и библиотека «Registry» для получения данных из файлов пассивного реестра, используемая в программе, написанные на языке программирования C#. Библиотека «Registry» является модификацией библиотеки с открытым исходным кодом, в которой была повышена производительность.

В данной программе было реализовано:

1. Определение и чтение файлов пассивного реестра;

2. Вывод связанной информации о сетевых интерфейсах;
3. Вывод связанной информации о сетевых картах;
4. Вывод связанной информации о сетевых подключениях;
5. Вывод связанной информации о USB носителях;
6. Вывод связанной информации о подключенных смартфонах;
7. Вывод связанной информации о подключенных принтерах;
8. Вывод связанной информации о портативных устройствах;
9. Вывод информации о подключенных устройствах;
10. Вывод информации о жестких дисках.

Эта глава содержит 9 подразделов. В разделе 3.1 «Работа с программой» рассказывается как работать с реализованной программой и о том, как она работает. На вход программы подается путь до папки, содержащей файлы пассивного реестра. После чего идет проверка на наличие файлов реестра по указанному пути. Файлы не обязательно должны иметь стандартное название, так как проверяются по сигнатуре в заголовке. После определения файлов происходит их разбор, где бинарные данные превращаются в ключи, ячейки и их списки, известные нам из главы 1. С помощью смещений они соединяются, образуя реестр Windows.

Последующие разделы содержат обзор режимов работы программы и анализ их работы, а именно:

1. 3.2 Вывод связанной информации о сетевых картах и интерфейсах;
2. 3.3 Вывод связанной информации о сетевых подключениях;
3. 3.4 Вывод связанной информации о USB носителях;
4. 3.5 Информация о портативный устройствах;
5. 3.6 Информация о подключенных устройствах;
6. 3.7 Информация о жестких дисках;
7. 3.8 Вывод связанной информации о подключенных смартфонах;
8. 3.8 Вывод связанной информации о подключенных смартфонах;
9. 3.9 Вывод связанной информации о подключенных принтерах.

ЗАКЛЮЧЕНИЕ

В данной работе мы подробно рассмотрели, что такое реестр Windows. Полностью разобрали его назначение, строение и расположение. Изучили и описали составляющие внутренней структуры реестра, такие как:

- Ключи;
- Списки подразделов;
- Списки значений;
- Записи безопасности;
- Значения.

Рассмотрели механизм следообразования в реестре Windows. Изучили основные ключи реестра, в которых могут содержаться следы при использовании аппаратного обеспечения и сетевых подключений, а также рассмотрели получение временных рамок их использования.

В ходе данной работы была разработана программа, способная выводить связанную информацию из файлов пассивного реестра Windows. Использование данной программы позволяет в разы увеличить скорость получения служебной информации, что ускоряет, соответственно, и поиск следов в компьютерных устройствах. Программа существенно экономит время и повышает эффективность работы эксперта, чем значительно улучшает ход расследования и упрощает разоблачение правонарушителя.