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

Установление обстоятельств создания файлов в разделе NTFS

АВТОРЕФЕРАТ
дипломной работы

студентки 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Гвоздевой Юлии Александровны

Научный руководитель
доцент, к. ю. н. _____ А. В. Гортинский
23.01.2020 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
23.01.2020 г.

Саратов 2020

ВВЕДЕНИЕ

Операционные системы Microsoft семейства Windows NT нельзя представить без файловой системы NTFS (от англ. New Technology File System – «файловая система новой технологии») – одной из самых сложных и удачных из существующих на данный момент файловых систем.

NTFS заменила использовавшуюся в MS-DOS и Microsoft Windows файловую систему FAT. NTFS поддерживает систему метаданных и использует специализированные структуры данных для хранения информации о файлах для улучшения производительности, надёжности и эффективности использования дискового пространства. NTFS хранит информацию о файлах в главной файловой таблице – Master File Table (MFT). NTFS имеет встроенные возможности разграничивать доступ к данным для различных пользователей и групп пользователей (списки контроля доступа – Access Control Lists (ACL)), а также назначать квоты (ограничения на максимальный объём дискового пространства, занимаемый теми или иными пользователями). NTFS использует систему журналирования для повышения надёжности файловой системы. [1, 7]

В данной работе будет рассмотрен поиск файлов пользователя по его SID (от англ. Security Identifier – идентификатор безопасности), поиск подозрительных файлов, определение разграничения доступа к файлам. Полученная информация, позволит несколько сократить время проведения компьютерно-технической экспертизы и повысить ее эффективность.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 92 страницы, из них 39 страниц – основное содержание, включая 43 рисунка и 2 таблицы, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

1 Структура и основные компоненты NTFS

1.1 Структура NTFS

Как и другие структуры файловых систем, структура NTFS, располагается в одном из разделов жесткого диска, указанном в таблице разделов. Первые шестнадцать секторов в разделе NTFS распределены под загрузочную запись и код загрузки (дубликат сектора загрузочной записи находится в логическом центре диска). [1]

NTFS память под файлы в разделе распределяет кластерами. Раздел NTFS условно делится на две части. И чтобы $MFT не фрагментировался при своем росте, первые 12,5% диска отводятся под так называемую MFT зону – пространство, в которое растет метафайл $MFT. Запись каких-либо данных в эту область невозможна. Остальные 87,5% диска представляют собой обычное пространство для хранения файлов. [16]

Свободное место диска, однако, включает в себя все свободное место, в том числе и незаполненные куски MFT–зоны.

Каждый элемент файловой системы NTFS представляет собой файл. NTFS является объектно-ориентированной файловой системой, и файл в NTFS – это набор атрибутов, которыми она манипулирует. [1, 2]

1.2 Метафайлы NTFS

NTFS включает несколько системных файлов (метафайлов), которые скрыты от просмотра на томе. Системные файлы используются только файловой системой для хранения метаданных и поддержания работы файловой системы. NTFS резервирует для метаданных первые 16 записей (около 1 Мб) в $MFT. Эти первые 16 файлов носят служебный характер и называются метафайлами, используемые в данный момент метафайлы и их назначение приведены в таблице 2. Остальные записи файла $MFT описывают файлы и каталоги. Метафайлы носят служебный характер. Каждый из них отвечает за какую-либо часть работы системы. [2-4, 11-12]

1.3 Структура записи $MFT

Основная информация о файле содержится в файловой записи (File Record) таблицы MFT, а небольшие файлы целиком хранятся в файловой записи.

Файловая запись состоит из заголовка (Header) и набора атрибутов (Attribute). В заголовке содержится служебная информация о файловой записи, например, её тип и размер. Все данные, относящиеся непосредственно к файлу, хранятся в виде атрибутов. Названия атрибутов также, как и системных файлов начинаются со знака "$". [4]

Каждый атрибут состоит из заголовка (attribute header), определяющего тип атрибута и его свойства, и тела (attribute body), содержащего основную информацию атрибута. [2-5, 15]

2 Понятие и структура SID

SID (от англ. Security Identifier – «Идентификатор безопасности») – это уникальный номер, идентифицирующий учетную запись пользователя, группы или компьютера. Он присваивается учетной записи при создании каждого нового пользователя системы. Внутренние процессы Windows обращаются к учетным записям по их кодам SID, а не по именам пользователей или групп. Если удалить, а затем снова создать учетную запись с тем же самым именем пользователя, то предоставленные прежней учетной записи права и разрешения не сохранятся для новой учетной записи, так как их коды безопасности будут разными. Аббревиатура SID образована от Security ID. [6]

Идентификатор SID представляет собой числовое значение переменной длины, формируемое из номера версии структуры SID, 48-битного кода агента идентификатора и переменного количества 32-битных кодов субагентов и/или относительных идентификаторов (Relative IDentifiers, RID). Код агента идентификатора определяет агент, выдавший SID, и обычно таким агентом является локальная операционная система или домен под управлением Windows. Коды субагентов идентифицируют попечителей, уполномоченных

агентом, который выдал SID, а RID – дополнительный код для создания уникальных SID на основе общего базового SID. [6-8, 17]

3 Защищенные ресурсы NTFS

3.1 Консолидированная безопасность в NTFS

NTFS всегда располагала функциями безопасности, позволяющими администратору указать пользователей, которым разрешен или запрещен доступ к тем или иным файлам и каталогам. В версиях NTFS, предшествовавших Windows 2000 (т.е. старше NTFS 3.0), дескриптор безопасности каждого файла и каталога хранился в его собственном атрибуте безопасности. Дескриптор безопасности – это специальная структура, которая хранит информацию о безопасности объекта. В Windows дескрипторы безопасности используются для описания политики контроля доступа, действующей в отношении файла или каталога. [13]

3.1.1 Атрибут $SECURITY_DESCRIPTOR

Атрибут $SECURITY_DESCRIPTOR в основном встречается в файловых системах Windows NT, потому что в NTFS версии 3.0 и далее этот атрибут сохраняется только для сохранения совместимости. В более старых версиях NTFS дескриптор безопасности файла хранился в атрибуте $SECURITY_DESCRIPTOR, обладающем идентификатором типа 0x50 в шестнадцатеричной системе счисления. В более новых версиях NTFS дескрипторы безопасности хранятся в одном файле, потому что многие файлы обладают одинаковым дескриптором безопасности, и было бы неэффективно хранить его в одном экземпляре для каждого файла. [18]

3.1.2 Файл $Secure

В NTFS версий 3.0+ дескрипторы безопасности хранятся в файле метаданных файловой системы $Secure.

Атрибут $STANDARD_INFORMATION любого файла или каталога содержит числовой код, называемый идентификатором безопасности (Security ID). Его значение используется для индексирования файла $Secure для поиска соответствующего

дескриптора. Идентификаторы безопасности уникальны только в рамках файловой системы, тогда как коды SID глобально-уникальны. [13, 18]

Файл $Secure содержит два индекса ($SDH и $SII) и один атрибут $DATA ($SDS). Атрибут $DATA содержит дескрипторы безопасности, а два индекса используются при ссылках на дескрипторы. Индекс $SII сортируется по идентификатору безопасности, хранящемуся в атрибуте $STANDARD_INFORMATION каждого файла. Индекс $SII используется для поиска дескриптора безопасности файла при известном идентификаторе безопасности. С другой стороны, индекс $SDH сортируется по хеш-коду дескриптора безопасности. [13-14, 18]

3.2 Обеспечение контроля доступа

Access Control List, или ACL – список контроля доступа, который определяет, кто или что может получать доступ к конкретному объекту и какие именно операции разрешено или запрещено этому субъекту проводить над объектом. ACL в системе представлены заголовком (ACL Header) и последовательностью элементов списка (ACE, Access-Control Entry). Их структура будет рассмотрена в следующем разделе.

ACL – это упорядоченный набор ACE (Access Control Entries – элементы управления доступом), которые определяют правила доступа, применимые к объекту и его свойствам. Каждый ACE определяет участника политики безопасности и устанавливает набор прав доступа, которые разрешены, запрещены или наблюдаются для данного пользователя. [8, 9]

3.2.1 Структура ACL

Структура ACL между версиями не изменяется, однако структура составляющих ее ACE может меняться. ACL представлен следующей структурой:

```
typedef struct _ACL {
BYTE AclRevision;
BYTE Sbz1;
WORD AclSize;
WORD AceCount;
WORD Sbz2;
} ACL;
```

Поле AclRevision содержит информацию о версии ACL.

Размер ACL (AclSize) определяет количество байт, выделенное под ACL, включая в себя заголовок ACL, все ACE и оставшееся место в буфере. Размер ACL меняется в зависимости от количества и размера его ACE. Максимальный размер ACL – 64 Кб, что приблизительно равно 1820 ACE, в зависимости от их размера.

Количество ACE (AceCount) в ACL может быть нулевым, из-за чего проверка доступа останавливается. [9]

3.2.2 Структура ACE

ACE (запись управления доступом) определяет способ взаимодействия SID с защищаемым объектом. Может разрешать или запрещать доступ для определенного SID. Структур ACE много, но структура у них похожа.

Каждая запись содержит SID того пользователя или группы, правило доступа для которого она определяет, маску доступа, определяющую описываемое правило доступа. Также она содержит набор флагов, которые определяют, могут или нет дочерние объекты наследовать эту запись ACE.

Поле Тип – начиная с версий Windows 2000 и 2003, поддерживает 6 типов ACE: три общих, которые могут быть присвоены любому защищаемому объекту, и три типа, которые нужны только для объектов Active Directory.

Маска доступа – 32-битное значение, которая и отвечает за доступ. Каждый бит может быть активен и неактивен, но его смысл будет зависеть от типа ACE. [9, 10]

4 Практическая часть

В рамках практического задания была создана программа на языке программирования C# с использованием Windows Forms – интерфейс программирования приложений, отвечающий за графический интерфейс пользователя. [19, 20] Реализован следующий функционал:

1) Получение схемы разрешений для каждого файла в выбранном каталоге, схема разрешений включает в себя такую информацию как права доступа, пользователя для которого заданы эти права, а также тип наследования разрешений.

2) Поиск файлов с выбранной схемой разрешения – это возможность пользователю выбирать самому, необходимые параметры для поиска файла с нужным ему разрешением.

3) Поиск подозрительных файлов – это возможность поиска следов, оставленных злоумышленником при вторжении в систему.

4) Поиск всех файлов выбранного владельца.

ЗАКЛЮЧЕНИЕ

NTFS – система, которая закладывалась на будущее, и это будущее для большинства реальных применений сегодняшнего дня, к сожалению, видимо еще не наступило. На данный момент NTFS обеспечивает стабильность и равнодушие к целому ряду факторов. Основное преимущество NTFS с точки зрения быстродействия заключается в том, что этой системе безразличны такие параметры, как сложность каталогов (число файлов в одном каталоге), размер диска, фрагментация.

Также в качестве практического задания была разработана программа для анализа файлов разделов NTFS по данным атрибутов. Она предназначена для быстрого поиска информации о каталогах и файлах, в которых может содержаться необходимая информация для следствия или экспертизы. Также были произведены эксперименты по использованию данной программы и по итогу их выполнения можно сделать следующие выводы:

1. Программа позволяет определять допустимые разрешения для доступа к файлу, как для зарегистрированных пользователей, так и для незарегистрированных пользователей. А также позволяет пользователю самому выбирать параметры для поиска файла с необходимой ему схемой разрешения.
2. Программа может помочь эксперту сократить время и усилия для поиска подозрительных файлов.
3. Программа позволяет определять зарегистрированных и незарегистрированных в системе пользователей, что может помочь эксперту в определении количества пользователей, использовавших данный жесткий диск.
4. Программа работает не только с файлами, созданными на данном жестом диске, но и с файлами, созданными на других внешних носителях.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Павлов, А. Ю. Методические указания Технологии доступа к данным в информационных системах: Файловая система NTFS. Часть II. / А. Ю. Павлов. – Самара: СамИИТ, 2002. – 22 с.

2 Thomas Schwarz, S. J. COEN 252 Computer Forensics NTFS [Электронный ресурс] : статья, открытый доступ / S. J. Thomas Schwarz // Santa Clara, California, 2007. – URL: http://www.cse.scu.edu/~tschwarz/coen252_07Fall/Lectures/NTFS.html (дата обращения: 10.09.2019). – Загл. с экрана. – Яз. англ.

3 Pascal Zachary, G. SHOWSTOPPER! The Breakneck Race To Create Windows NT And the Next Generation at Microsoft. – 1994. – 312 с.

4 Кастер, Х. М. Основы Windows NT и NTFS/Пер. с англ. – М.: Издательский отдел «Русская редакция» ТОО «Chanel Trading Ltd», 1996. – 440 с.

5 Файловая система NTFS. [Электронный ресурс] : образовательный портал. – URL: https://www.intuit.ru/studies/courses/10471/1078/lecture/16586 (дата обращения: 01.10.2019). – Загл. с экрана. – Яз. рус.

6 Технический обзор идентификаторов безопасности [Электронный ресурс] : статья, открытый доступ. – URL: https://technet.microsoft.com/ru-ru/library/dn743661(v=ws.11).aspx (дата обращения 14.10.19). – Загл. с экрана. – Яз. рус.

7 Файловая система NTFS [Электронный ресурс] : статья, открытый доступ. – URL: http://www.ixbt.com/storage/ntfs.html (дата обращения 20.10.19). – Загл. с экрана. – Яз. рус.

8 Идентификаторы учетных записей в Windows 2000 / XP / 2003 / VISTA [Электронный ресурс] : статья, открытый доступ. – URL: http://ntinside.narod.ru/sid.html (дата обращения 29.10.19). – Загл. с экрана. – Яз. рус.

9 How the System Uses ACLs [Электронный ресурс] : статья, открытый доступ. – URL: http://www.ntfs.com/ntfs-permissions-acl-use.htm (дата обращения: 04.11.2019). – Загл. с экрана. – Яз. англ.

10 Russon, R., Fledel, Y. NTFS Documentation [Электронный ресурс] : статья, открытый доступ / R. Russon, Y. Fledel. – URL: http://ftp.kolibrios.org/users/Asper/docs/NTFS/ntfs doc.html (дата обращения: 13.11.2019). – Загл. с экрана. – Яз. англ.

11 Кэрриэ, Б. Криминалистический анализ файловых систем / Б. Кэрриэ – СПб.: Питер, 2007. – 480 с.: ил.

12 Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP и Windows 2000. Мастер класс. / Пер. с англ. — 4-е изд. СПб.: Питер, 2008. 992 стр.: ил.

13 Касперски, К. Файловая система NTFS извне и изнутри Часть 1 [Электронный ресурс] : статья, открытый доступ / К. Касперски. – URL: http://samag.ru/archive/article/375 (дата обращения: 27.11.2019). – Загл. с экрана. – Яз. англ.

14 Касперски, К. Файловая система NTFS извне и изнутри Часть 2 [Электронный ресурс] : статья, открытый доступ / К. Касперски. – URL: http://samag.ru/archive/article/395 (дата обращения: 27.11.2019). – Загл. с экрана. – Яз. рус.

15 Руссинович, М., Соломон, Д. Внутреннее устройство Microsoft Windows. – СПб.: Питер, 2013. – 800с.: ил.

16 Побегайло, А. П. Системное программирование в Windows. – СПб.: БХВ-Петербург, 2006. – 1056 с.: ил.

17 Хорошо известные идентификаторы безопасности в операционных системах Windows [Электронный ресурс] : статья, открытый доступ. – URL: https://support.microsoft.com/ru-ru/help/243330/well-known-security-identifiers-in-windows-operating-systems (дата обращения 28.11.19). – Загл. с экрана. – Яз. рус.

18 Безопасность объектов Windows [Электронный ресурс] : электронная библиотека. – URL: http://www.uhlib.ru/kompyutery_i_internet/sistemnoe_programmirovanie_v_srede_windows/p16.php (дата обращения 30.11.19). – Загл. с экрана. – Яз. рус.

19 Рихтер, Д. CLR via C#. Программирование на платформе Microsoft .NET Framework 4.5 на языке C#. 4-е изд, 2018, 896 с.

20 Сведения о Windows Forms [Электронный ресурс] : открытая документация. – URL: https://docs.microsoft.com/ru-ru/dotnet/framework/winforms/windows-forms-overview (дата обращения 25.09.19). – Загл. с экрана. – Яз. рус.