МЕТОДЫ СОКРЫТИЯ ИНФОРМАЦИИ В ФАЙЛОВОЙ СИСТЕМЕ NTFS

О. Р Мысливец
Факультет математики и информатики, Гродненский государственный университет имени Янки Купалы
Гродно, Республика Беларусь
E-mail: myslivec.oleg@yandex.ru

В данной работе исследуются методы сокрытия информации в файловой системе NTFS. Исследуются особенности этих методов и их специфика согласно существующим критериям эффективности методов сокрытия информации для файловых систем.

Введение

Широкая распространенность NTFS привела к тому, что данная файловая система наиболее часто подвергается криминалистическому анализу с целью обнаружения доказательств преступления. Однако, извлечь необходимые данные не всегда легко. В первую очередь это связано с компьютерной грамотностью злоумышленника и теми методами, которые он использовал. Наряду со стандартными методами анти-форензики [1], такими как криптография и стеганография, существует возможность использовать структуру самой файловой системы для сокрытия информации.

I. Критерии эффективности методов сокрытия информации для файловых систем

Методы сокрытия информации для файловых систем должны удовлетворять следующим очевидным критериям [2]:

- Стандартные средства проверки файловой системы не должны возвращать никаких ошибок;
- Сокрытие данные не должны быть перезаписаны или вероятность их перезаписи должна быть минимальной;
- Сокрытие данные не должны отображаться стандартными GUI — интерфейсами ОС;
- Метод должен позволять скрывать разумный объем данных.

Метод, который не удовлетворяет более чем одному из этих условий должен считаться неэффективным в перспективе долгосрочного хранения данных, а в противном случае метод можно считать эффективным.

II. Методы сокрытия информации в файловой системе NTFS

Первым возможным эффективным методом сокрытия информации в файловой системе NTFS является сокрытие данных в фиктивных поврежденных кластерах. В NTFS поврежденные кластеры помечаются в метафайле $BadClus. Существует возможность пометить в данном метафайле некоторые кластеры как поврежденные и записать в них необходимое количество информации.

Если при проведении криминалистического анализа возникло подозрение, что используется данный метод сокрытия информации, то проверить правильность догадки не составляет особых трудностей: для этого достаточно провести сканирование поверхности жесткого диска. После достаточно сравнить результаты работы процедуры сканирования с результатами анализа файловой системы NTFS на наличие отмеченных поврежденных кластеров. Если использовать жесткий диск не представляется возможным, то одним из возможных вариантов является попытка извлечения данных из таких кластеров с последующим восстановлением полученных данных. Следует заметить, что если обнаружение факта сокрытия информации данным способом не вызывает особой сложности, то извлечение данных может быть сопряжено с рядом проблем, например, злоумышленник может предварительно зашифровать данные или удалить файловые сигнатуры для предотвращения обнаружения сокрытых данных. Данный метод сокрытия информации можно считать эффективным, так как он удовлетворяет всем четырем критериям эффективности.

Вторым возможным эффективным методом сокрытия информации является выделения дополнительных кластеров для файла и их использование. С помощью данной техники возможно сокрытие данных произвольного размера, так как злоумышленник может дополнительно выделить любое возможное количество секторов. С позиции злоумышленника можно выделить единственный недостаток данного метода: данные могут быть потеряны, если файл изменяется в размере. Решением данной проблемы может быть использование файлов, размер которых не будет изменяться.

Данный метод сокрытия информации легко обнаружить, проведя сканирование утилитой проверки файловой системы или начать анализ с проверки количества выделенных секторов для файла с реальным размером файла. Самый быстрый способ получить необходимые значения – извлечь их из заголовка атрибута $DATA. Ес-

ли неиспользуемое файлом место больше размера кластера, то можно судить о том, что в выделенных для файла кластерах содержатся данные для последующего анализа.

Метод сокрытия информации на основе выделения дополнительных кластеров можно считать эффективным, хотя он и не удовлетворяет одному из требований эффективности. Однако, следует заметить, что несмотря на довольно легкий способ обнаружения использования данного метода, использование стандартных методов анти-форензики вместе с данной техникой может существенно осложнить работу эксперта-криминалиста.

Третьим эффективным методом сокрытия информации является использование альтернативных потоков данных NTFS. Размер данных, которые могут скрыты с помощью этой технологии, может быть произвольным. Данная техника является самой простой в использовании, так как не требует специального программного обеспечения и манипуляций с файловой системой на низком уровне. Дополнительной проблемой при анализе данных в альтернативных потоках NTFS является тот факт, что альтернативные потоки зачастую используются и в законных целях. Из этого следуют следующие для злоумышленника возможности, которые должны быть учтены экспертом-криминалистом при анализе альтернативных потоков данных:

- Изначально требуется определить используется ли альтернативный поток данных для скрытия информации или он используется в законных целях, что может быть проблематично, если злоумышленник дополнительно использует другие методы анти-форензики;
- Злоумышленник может использовать название потока, которое использует любая легитимная программа, для предотвращения обнаружения.

Учитывая все особенности данного метода сокрытия информации и тот факт, что эта техника удовлетворяет всем критериям эффективности, можно считать альтернативные потоки данных NTFS эффективным методом сокрытия информации.

Четвертым эффективным методом сокрытия информации является сокрытие данных, используя extended attribute или $EA [3]. Изначально данный атрибут был необходим для совместимости с приложениями OS/2, однако в настоящее время в ОС семейства Windows данный атрибут не используется. Этот факт позволяет использовать $EA для сокрытия данных. Атрибут может иметь переменную длину, однако, его максимальный размер равен 65536 байтам. Во всем остальном функционал данного атрибута схож с функционалом альтернативных потоков данных, за исключением того, что для манипуляций с $EA необходимо специальное программное обеспечение. Данный метод удовлетворяет всем критериям эффективности и также может считаться эффективным методом сокрытия информации.

III. Заключение

Файловая система NTFS имеет очень эффективную и одновременно сложную структуру. Однако, именно сложная структура NTFS позволяет эффективно использовать множество разнообразных методов сокрытия информации, каждый из которых может найти свое применение на практике. Знание особенностей исследуемой файловой системы, возможных методов сокрытия информации в NTFS, их эффективности и специфики позволит экспертам криминалистам проводить более эффективный криминалистический анализ данной файловой системы.

Список литературы

1. Anti-forensic techniques [Электронный ресурс] / ForensicsWiki – Режим доступа: http://www.forensicswiki.org/wiki/Anti-forensic_techniques. – Дата доступа: 08.09.2016
2. Detecting steganographic content on the internet [Электронный ресурс] / Computer Systems Laboratory Colloquium – Режим доступа: https://web.stanford.edu/class/ee380/Abstracts/011107.html – Дата доступа: 08.09.2016
3. Linux NTFS Project [Электронный ресурс] / $EA (0xE0) - Attribute - NTFS Documentation– Режим доступа: https://flatcap.org/linux-ntfs/ntfs/attributes/ea.html – Дата доступа: 08.09.2016