УДК 343.98 DOI: 10.18698/2541-8009-2023-7-919

КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМАЯ ИНФОРМАЦИЯ, СОДЕРЖАЩАЯСЯ В АЛЬТЕРНАТИВНЫХ ПОТОКАХ ДАННЫХ

В.А. Писанова viktorija-pisanova@rambler.ru

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Рассмотрены понятие и сущность альтернативных потоков данных. Выделены признаки, делающие альтернативные потоки удобным инструментом для злоумышленников. Установлено, что альтернативные потоки данных могут быть использованы для сокрытия данных как самим пользователем, так и для хранения несанкционированной пользователем информации. Рассмотрены конкретные примеры криминалистически значимой информации, которая может содержаться в альтернативных потоках данных. Сделан вывод о том, что альтернативные потоки могут иметь большое значение для раскрытия, расследования и предупреждения преступлений, в связи с чем им следует уделять особое внимание в ходе проведения компьютерно-технической экспертизы.

Ключевые слова

Специальные знания, судебная экспертиза, компьютерные технологии, файловая система, альтернативные потоки данных, скрытая информация, криминалистически значимая информация, компьютерно-техническая экспертиза

Поступила в редакцию 29.06.2023

Целью данной работы является изучение криминалистически значимой информации, которая может содержаться в альтернативных потоках данных. Для реализации указанной цели были поставлены следующие задачи:

– изучить структуру и особенности файловой системы NTFS;

– рассмотреть понятие и сущность альтернативных потоков данных;

– изучить виды информации, которая может содержаться в альтернативных потоках данных и дать оценку ее важности для нужд раскрытия, расследования и предотвращения преступлений.

Файловая система — это программа, обеспечивающая логическое размещение и хранение данных и команд на машинных носителях информации в виде логических дисков, папок (каталогов) и файлов [1, с. 101] На сегодняшний день бóльшая часть электронных носителей информации, используемых в качестве внутренней памяти в персональных компьютерах и ноутбуках, имеет файловую систему NTFS.

В файловой системе NTFS каждый из файлов фактически представляет собой набор потоков, хранящих данные. Обычно все данные находятся в основном потоке, однако специфика файловой системы NTFS такова, что позволяет

добавлять к файлу и дополнительные потоки, получившие название «альтернативные потоки данных» (оригинальное название Alternate Data Streams, или ADS). Поддержка альтернативных потоков появилась достаточно давно и была реализована в NTFS для совместимости с другими файловыми системами, например, HFS, хранившая данные о файле в специальном потоке [2].

Потоки данных в файловой системе NTFS являются дополнительными свойствами атрибута $DATA. По умолчанию существует единственный неименованный поток $DATA:. Однако при необходимости могут быть созданы и дополнительные поименованные потоки, которые будут иметь вид *НазваниеПотока1:$DATA* и являться альтернативными [3].

Таким образом, у каждого файла или каталога в NTFS может быть несколько потоков данных, содержимое которых никак не связано между собой. Даже размер альтернативного потока может превышать размер основного. Еще одной важной особенностью альтернативного потока является то, что размер помещенных в альтернативный поток данных не увеличивает видимый объем файла, однако объем места, занимаемого файлом на диске, увеличивается с учетом размера альтернативных потоков.

По умолчанию все записываемые в файл данные попадают в основной поток. Именно его видит пользователь, открывая файл стандартными средствами, в то время как содержимое и даже сам факт наличия альтернативных потоков скрыты от большинства приложений, предназначенных для управления файлами. Для поиска и чтения данных, содержащихся в альтернативных потоках, можно использовать специальное программное обеспечение или стандартные возможности, предоставляемые операционной системой [4, с. 423].

Альтернативные потоки сохраняются при копировании и перемещении файла на другой накопитель, но лишь в том случае, если он также имеет файловую систему NTFS.

В альтернативных потоках может содержаться информация любого типа, в том числе текст, видео, аудио, графические изображения и исполняемые файлы, причем работа с ней возможна напрямую, без предварительного извлечения из альтернативного потока.

Таким образом, можно выделить несколько важных признаков альтернативных потоков:

– скрытость — для обнаружения альтернативного потока необходимо воспользоваться специализированными утилитами или специальными командами встроенных утилит;

– отсутствие ограничений на тип и размер хранимой информации [5].

Указанные выше признаки делают альтернативные потоки удобным инструментом для сокрытия данных, вредоносных программ и действий злоумышленников, а также объектом интереса компьютерно-технического эксперта — лица, обладающего специальными знаниями, которому в установленном

законом порядке поручено проведение экспертизы и процессуальной фигуры, чей статус регламентирован законом [6].

Фактически функция альтернативных потоков такова, что позволяет пользователю скрыть значительное количество данных, а также хранить в файловой системе несанкционированную пользователем информацию. По своей сути альтернативные потоки являются легитимной функцией файловой системы NTFS, однако специфика их функционирования такова, что они представляют собой удобную нишу для действий злоумышленников. Все это делает альтернативные потоки данных важным источником криминалистически значимой информации, который должен быть соответствующим образом исследован экспертом при проведении компьютерно-технической экспертизы.

Как уже упоминалось ранее, в альтернативных потах может содержаться информация абсолютно любого типа, причем она может создаваться как самим пользователем, так и различными программами.

Что касается санкционированных данных, то альтернативные потоки могут быть использованы для хранения некоторой сопутствующей информации о файле. Это могут быть ключевые слова, краткая информация о файле, ассоциируемые с файлом звук и/или шрифт, инфраструктура классификации файлов [7] и т. д. Альтернативные потоки добавляются браузером к файлам, скачанным из сети Интернет. Он имеет название ZoneIdentifier и содержит признак секции с описанием зоны передачи данных (ZoneTransfer) и идентификатор зоны (ZoneId), обозначающий в числовом виде одну из пяти зон безопасности, в зависимости от того, откуда файл был получен. Так, цифра 0 обозначает локальный компьютер, 1 — местную сеть, 2 — надежный сайт, 3 — Интернет, а 4 — опасные сайты [2]. Эти обозначения использует, например Microsoft Office, выдавая при открытии файла соответствующие предупреждения. Также в этом альтернативном потоке может содержаться адрес сайта, с которого был скачан файл. Такая информация может содержаться, например, в альтернативных потоках файлов, скачанных из социальной сети «ВКонтакте».

Некоторые многофункциональные устройства, например фирмы Hewlett Packard, создают альтернативные потоки в файлах отсканированных документов, в которые помещаются сведения о модели устройства, на котором проводилось сканирование. Как уже упоминалось выше, сведения в альтернативных потоках могут быть легко изменены или полностью удалены, в связи с чем при оценке достоверности сведений, полученных из альтернативных потоков, следует соотносить их со сведениями из других источников.

Просмотрев содержащиеся в альтернативном потоке файла сведения, можно сделать предположение о его происхождении. Однако данная информация не может считаться в полной мере достоверной, поскольку содержимое альтернативного потока может быть изменено вручную или же он может быть полностью удален.

Также альтернативные потоки могут быть использованы антивирусными программами, например антивирусом Касперского, для хранения там рассчитанной контрольной суммы, полученной по итогам проверки системы [5].

Альтернативные потоки могут быть широко использованы для намеренного сокрытия информации, поскольку помещенные в альтернативный поток данные становится фактически невидимыми для рядового пользователя. Таким образом могут быть спрятаны значительные объемы запрещенной законом информации (видео- и аудиофайлы, содержащие призывы к осуществлению экстремистской и/или террористической деятельности, детская порнография и проч.), а также сведения, напрямую связанные с осуществлением противозаконной деятельности (неправомерно полученная компьютерная информация, местоположения наркотических средств, заготовки для последующей фальсификации денежных билетов и проч.) [3].

Отдельно необходимо упомянуть про использование альтернативных потоков вредоносным программным обеспечением. Одним из наиболее распространенных способов является помещение файлов вредоносной программы в альтернативные потоки данных существующих на атакуемом компьютере файлов или каталогов. Другим вариантом служит заражение компьютера путем передачи на него файла, содержащего альтернативный поток с вредоносной программой.

Вредоносная программа может при первом запуске присоединяться в качестве альтернативного потока к системной папке Windows и продолжает действовать уже оттуда. Так, ведет себя VirTool:Win32/Rustock.A и некоторые другие вредоносные программы этого семейства [8].

Некоторые вредоносные программы распространяются путем копирования себя в основной поток файлов с предварительным перемещением его первоначального содержимого в альтернативный поток. То есть в некоторых случаях сам факт наличия альтернативного потока может свидетельствовать о том, что устройство подвергалось воздействию вредоносной программы.

Таким образом, в альтернативных потоках может содержаться большое количество разнообразной информации, которая может иметь криминалистическую значимость. В связи с этим при проведении компьютерно-технических экспертиз следует обращать внимание на альтернативные потоки данных и потенциально содержащиеся в них сведения, необходимые для раскрытия расследования и предотвращения преступлений.

Видится необходимым проводить поиск альтернативных потоков на всех поступивших на исследование электронных носителях информации, в первую очередь в целях обнаружения тех потоков, которые были созданы пользователем. Вместе с тем чтение содержимого каждого альтернативного потока и оценка важности его содержимого в рамках конкретного экспертного исследования будут слишком длительным и трудоемким процессом. Для оптимизации этого

процесса эксперт может использовать специализированные программы, направленные на поиск и извлечение данных из альтернативных потоков, например AlternateStreamView [9] или NTFS Stream Explorer [10]. Указанные программы отвечают экспертным задам и позволяют выделить альтернативные потоки, потенциально содержащие криминалистически значимую информацию, и оперативно изучить их содержимое. Для указанных целей так же отлично подходят экспертное программное обеспечение такое, как например EnCase Forensic Edition или Autopsy.

Вместе с тем необходимо отметить, что значимость информации, содержащейся в альтернативных потоках информации для раскрытия, расследования и предотвращения преступлений во многом будет зависеть от существа дела и стоящих перед экспертом вопросов. Наибольшую пользу содержимое альтернативных потоков может принести в случаях, когда они были использованы злоумышленником для сокрытия информации. Во всех остальных случаях содержимое альтернативных потоков служит скорее косвенным указанием на некоторые действия программ и/или пользователей и будет иметь высокую криминалистическую значимость лишь в совокупности с иными цифровыми следами.

Литература

[1] Вехов В.Б., Зуев С.В., ред. *Цифровая криминалистика*. Москва, Юрайт, 2021, 417 с.

[2] *Заметки о Windows. Альтернативные потоки данных в NTFS*. URL: https://windowsnotes.ru/other/alternativnye-potoki-dannyx-v-ntfs/ (дата обращения 14.05.2023).

[3] Соколов А.Б., Щербина Р.П., Шаевич А.А. Криминалистически значимая информация, хранящаяся в альтернативных потоках данных файловой системы NTFS. *Криминалистика: вчера, сегодня, завтра*, 2022, т. 22, № 2, с. 159–169. http://doi.org/10.55001/2587-9820.2022.88.70.016

[4] Долгушина П.Е., Караваева А.В., Молодцова Ю.В. Возможности исследования альтернативных потоков данных. *Modern Science*, 2022, № 4–1, с. 422–426.

[5] Долгушина П.Е., Караваева А.В., Молодцова Ю.В. Альтернативные потоки данных в файловой системе NTFS. *Инновационные процессы в науке, технике и экономике. Междунар. науч.-практ. конф.: сб. тр. В 2. ч.* Тюмень, ТИУ, 2022, ч. 1, с. 94–98.

[6] Лядовская Н.И., Писанова В. А. Особенности специальных знаний при производстве судебной компьютерно-технической экспертизы. *Политехнический молодежный журнал*, 2022, № 10 (75). http://doi.org/10.18698/2541-8009-2022-10-830

[7] *Альтернативные потоки данных NTFS, или почему не запустился скрипт PowerShell*. URL: https://www.outsidethebox.ms/17918/ (дата обращения 20.05.2023).

[8] *Microsoft Security Intelligence*. URL: https://www.microsoft.com/en-us/wdsi/threats (accessed May 13, 2023).

[9] *AlternateStreamView v1.56*. URL: https://www.nirsoft.net/utils/alternate_data_streams.html (accessed May 17, 2023).

[10] *Обзор программы NTFS Stream Explorer*. URL: https://clck.ru/fDti2 (дата обращения 17.05.2023).

Писанова Виктория Алексеевна — студентка кафедры «Безопасность в цифровом мире», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Тарасов Дмитрий Александрович, старший преподаватель кафедры «Безопасность в цифровом мире», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:
Писанова В.А. Криминалистически значимая информация, содержащаяся в альтернативных потоках данных. *Политехнический молодежный журнал*, 2023, № 07 (84). http://dx.doi.org/10.18698/2541-8009-2023-7-919

FORENSICALLY SIGNIFICANT INFORMATION CONTAINED IN THE ALTERNATIVE DATA STREAMS

V.A. Pisanova viktorija-pisanova@rambler.ru

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The article considers the concept and essence of the alternative data flows. Specific indicators are highlighted making it possible to transform the alternative streams into a convenient tool for intruders. It was established that alternative data streams could be used to hide data both by the user himself and also to store information unauthorized by the user. Specific examples of forensically significant information that could be contained in the alternative data streams were analyzed. A conclusion was made that alternative streams could be of great importance for detection, investigation and prevention of crimes; therefore, special attention in the course of computer forensics should be paid to them.

Keywords

Special knowledge, forensic examination, computer technology, file system, alternative data streams, hidden information, forensically significant information, computer forensics

Received 29.06.2023

References

[1] *Tsifrovaya kriminalistika* [Digital forensics]. Ed. Vekhov V.B., Zuev S.V. Moscow, Yurayt Publ., 2021, 417 p. (In Russ.).

[2] *Zametki o Windows. Al'ternativnye potoki dannykh v NTFS* [Notes on Windows. Alternate Data Streams in NTFS]. URL: https://windowsnotes.ru/other/alternativnye-potoki-dannyx-v-ntfs/ (accessed May 05, 2023).

[3] Sokolov A.B., Shcherbina R.P., Shaevich A.A. Criminally significant information stored in alternative data streams of the NTFS file system. *Forensics: yesterday, today, tomorrow*, 2022, vol. 22, no. 2, pp. 159–169. (In Russ.). http://doi.org/10.55001/2587-9820.2022.88.70.016

[4] Dolgushina P.E., Karavaeva A.V., Molodtsova Yu.V. Opportunities to explore alternative data streams. *Modern Science*, 2022, no. 4–1, pp. 422–426. (In Russ.).

[5] Dolgushina P.E., Karavaeva A.V., Molodtsova Yu.V. Alternative data streams in the NTFS file system. *Innovatsionnye protsessy v nauke, tekhnike i ekonomike. Mezhdunar. nauch.-prakt. konf.: sb. tr.* [Innovation processes in science, technology and economics. International scientific-practical conference: collection of works]. Tyumen, IUT Publ., 2022, pt. 1, pp. 94–98. (In Russ.).

[6] Lyadovskaya N.I., Pisanova V.A. Opportunities for minors to file a statement of claim. *Politekhnicheskiy molodezhnyy zhurnal*, 2022, no. 10 (75). (In Russ.). http://dx.doi.org/10.18698/2541-8009-2022-10-830.html

[7] *Al'ternativnye potoki dannykh NTFS, ili pochemu ne zapustilsya skript PowerShell* [Alternative NTFS data streams, or why the PowerShell script didn't run]. URL: https://www.outsidethebox.ms/17918/ (accessed May 20, 2023).
[8] *Microsoft Security Intelligence*. URL: https://www.microsoft.com/en-us/wdsi/threats (accessed May 13, 2023).
[9] *AlternateStreamView v1.56*. URL: https://www.nirsoft.net/utils/alternate_data_streams.html (accessed May 17, 2023).
[10] *Obzor programmy NTFS Stream Explorer* [Overview of NTFS Stream Explorer]. URL: https://clck.ru/fDti2 (accessed May 05, 2023).

Pisanova V.A. — Student, Department of Security in the Digital World, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Tarasov D.A., Senior Lecturer, Department of Security in the Digital World, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Pisanova V.A. Forensically significant information contained in the alternative data streams. *Politekhnicheskiy molodezhnyy zhurnal*, 2023, no. 07 (84). (In Russ.).
http://dx.doi.org/10.18698/2541-8009-2023-7-919