СЛЕДЫ КИБЕРПРЕСТУПЛЕНИЙ

Зайцев А.А., Смолин А.В.
Нижегородская академия МВД России, г. Нижний Новгород
email: alexej.zaitseff2011@yandex.ru

Аннотация. в статье рассматриваются механизм следообразования «виртуальных следов преступлений», совершенных с применением компьютерной техники, виды «виртуальных следов», особенности их обнаружения. Также уделяется внимание некоторым способам совершения киберпреступлений.

Ключевые слова: следователь, киберпреступность, виртуальный след, компьютерная техника, информация, программное обеспечение.

Цифровые технологии приобрели популярность еще в 80-х годах прошлого столетия, а с появлением информационно-телекоммуникационных сетей нашу жизнь без них трудно себе представить. Однако, вместе с положительными моментами применения компьютерной техники и информационно-телекоммуникационных сетей, имеют место и отрицательные. Чем выше уровень развития компьютерных технологий, тем чаще они используются при совершении преступлений.

Все преступления в сфере высоких технологий объединяются общим термином – киберпреступность. Под этим понятием В.А. Номоконов и Т.Л. Тропинина понимали совокупность преступлений, совершаемых в киберпространстве с помощью, посредством или против компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству [1, с. 48].

Особенностью преступлений совершенных с применением компьютерной техники является то, что основными носителями информации о совершенном деянии являются виртуальные следы. В основе механизма образования виртуальных следов находятся электромагнитные взаимодействия двух и более материальных объектов – объективных форм существования (представления) компьютерной информации [2, с. 28-29]. Для обнаружения виртуальных следов необходимо наблюдать за различиями формы компьютерной информации: содержания, формата и других характеристик, алгоритма работы программы, автоматически создаваемых программой скрытых файлов. Происходящие изменения и будут являться следами-отображениями.

Объектами следообразования будут выступать файлы, программное обеспечение в виде баз данных и т.п., интернет-сайты, электронные информационные базы данных, электронные сообщения и документы [3].

И конечно, очевидным представляется, что следами-предметами в рассматриваемой нами категории преступлений будут являться как сами компьютеры с имеющимися в них микросхемами и составными частями, так и пластиковые карты, средства мобильной связи и т.п. Указанные объекты только тогда имеют значение, когда в них находится информация, непосредственно связанная с интересующим следствие событием и имеющая доказательственное значение.

Виртуальные следы можно классифицировать по различным основаниям. Так, по месту образования виртуальные следы подразделяются на следы на компьютерном устройстве преступника и на следы на компьютерном устройстве «жертвы» [4]. Кроме того, данные следы могут быть первичными и вторичными: первичные следы – это следы, образующиеся от непосредственного воздействия пользователя с использованием какой-либо информационной технологии. Вторичные же следы образуются вследствие технологических процессов без участия человека и вне желания последнего [5].

К «виртуальным следам» относятся:

- программы и файлы (возможно оставшиеся частично), не функционирующие на компьютерной технике до момента совершения преступления;
- умышленно занесенные злоумышленником для изменения характеристик системы символы, знаки и команды, находящиеся в различных программах;
- log-файлы, содержащие информацию о пользователях устройства.

Необходимо учитывать, что любые операции с компьютерной техникой, со средствами мобильной связи и т.п., находят отражение в памяти указанных устройств, а именно:

- включение и выключение устройства, операции с информацией в памяти компьютерного устройства находят свое отображение в журналах администрирования;
- манипуляции с программами находят свое отражение в реестре компьютерной техники;
- сведения о работе в информационно-телекоммуникационной сети «Интернет», а также в локальных сетях находят отражение в log-файлах;
- операции с файлами находят отражение в свойствах файлов [6].

Обнаружить виртуальные следы возможно, как на материальных объектах, так и на нематериальных: на ресурсах информационно-телекоммуникационной сети «Интернет», в различных социальных сетях, в платежных электронных («Яндекс.Деньги», «Qiwi-кошелек», и т.п.), в информационных базах данных (ГИБДД и т. п.), в локальных сетях различных учреждений, на винчестерах компьютерных устройств, на «флэш-картах», устройствам связи и других.

Следообразующие объекты будут зависеть от этапа совершения преступления с использованием компьютерных устройств. Основными характеристиками следообразующих объектов являются:

- размер программного обеспечения и электронных сообщений;
- время и даты создания (изменения) файлов и сообщений;
- некоторые характеристики (признаки скрытого или системного файла и т.п.) файлов и сообщений;
- отличительные фрагменты файлов или программ, позволяющие определить вредоносную программу.

Привлекает внимание обмен информацией с использованием так называемых «файлообменников». Последние представляют собой промежуточные серверы, применяющиеся для хранения определенного объема информации. При этом «файлообменники» создают ссылку на скачивание информации, размещенной пользователем. При этом, объект, содержащий ту или иную информацию, на интернет-сайте не размещается, а имеется только ссылка на него. Проще говоря, «файлообменник» – это промежуточное звено, который через информационно-телекоммуникационную сеть «Интернет» предоставляет доступ к информации, обеспечивая ее обмен. На данные звенья пользователи помещают большой объем информации, после чего делятся ссылками.

В настоящее время «файлообменики» уступили лидирующее место в данной области «торрент-трекерам», которые в основном не требуют регистрации пользователя. Распространение путем использования «торент-трекеров» приняло угрожающие масштабы, поскольку использует технологию (peer-to-peer), когда любое компьютерное устройство с указанным программным обеспечением, может стать местом хранения информации, а следовательно, и следов преступления, к которому имеется свободный доступ для получения информации другими компьютерными устройствами, с аналогичным программным обеспечением. Передача информации в этом случае идет в двух направлениях.

Возможность установления виртуальных следов в информационно-телекоммуникационной сети «Интернет» у следователя выражается также в

следующем: существующая в информационно-телекоммуникационной сети «Интернет» служба «Whois», обладает возможностями установления провайдера, предоставившего злоумышленнику, совершившему то, или иное деяние, доступ в «Интернет». Контакт с «Whois» осуществляется через сервис, расположенный по адресу: www.ripe.net. Дату и время, а также продолжительность выхода в информационно-телекоммуникационную сеть необходимо установить уже у провайдера по ведущемуся у него log-файлу.

Аналогично возможно определить рабочее место злоумышленника по log-файлу сервера локальной сети.

Как указывалось выше, все сеансы в информационно-телекоммуникационной сети «Интернет» автоматически отражаются в протоколе выхода на каждом компьютерном устройстве, однако при этом количество дней хранения данной информации определяется пользователем данного компьютерного устройства. Абсолютно логично, что полное совпадение информации, содержащейся в вышеуказанном протоколе с информацией из log-файла провайдера будет являться великолепным доказательством.

Что же касается следов в электронной почте, то необходимо отметить, что данные о пользователе электронного почтового ящика (анкетные данные, место работы и фото, а также т.п.) не всегда совпадают с действительностью, однако иногда бывают достоверны.

Нельзя обойти стороной и сеансы в «Интернете» через программное обеспечение «месенджеров» и т.п. Имея большую информационную и доказательственную ценность, вся информация о данных контактах и их содержание автоматически сохраняется в так называемых временных файлах. Последние, даже после их удаления, могут быть восстановлены.

Следует отметить, что многие программы фирмы «Microsoft» создают резервные копии файлов, файлы-отчеты, сохраняют информацию о последних проделанных операциях и выполненных программах, а также содержат иную информацию, представляющую огромный интерес для расследования.

Самым распространенным способом совершения преступлений с использованием компьютерной техники и программного обеспечения является применение вредоносных компьютерных программ. Последние, как правило, используются для незаконного получения различной, в том числе конфиденциальной, информации. Как ранее указывалось, следообразующие объекты, при совершения деяния данного вида, будут зависеть от этапа совершения преступления.

Начальным этапом рассматриваемого деяния будет внедрение вредоносной программы. Как правило, это электронное сообщение, содержащее прикрепленный файл в специальном формате, к которым после активизации прибавится исполняемый файл. Соответственно, криминалистически важное значение будет иметь изменение характеристик следообразующих объектов:

- увеличение или уменьшение размеров программ и появление электронных сообщений с присоединенным файлом;
- дата и время получения и создания, а также изменения модификации файлов и сообщения;
- отдельные свойства вышеуказанного файла и сообщения;
- отдельные свойства программ или файлов конфигурации, позволяющие определить конкретную вредоносную программу [7].

Кроме файлов вышеуказанной следообразующими также будут являться:

- файлы, использующиеся для электронной рассылки;
- файлы, использующиеся для создания вредоносной программы, содержащие информацию о ее версии, ее настройки и свойства.

Как уже указывалось, в данном случае при совершении преступления, сопряженного с вредоносными программами, будет использовано как минимум два компьютерных устройства, а именно первый будет принадлежать злоумышленнику, а второй будет принадлежать пострадавшей стороне. На компьютерном устройстве пострадавшей стороны следообразующими объектами будет таблица размещения файлов (FAT, NTFS или другая в зависимости от типа используемой операционной системы), а также файлы с программами, являющимися первой частью вредоносной программы. Чаще всего это исполняемый файл (так сказать сама программа), и еще файл, содержащий свойства конфигурации и вспомогательные данные, необходимые для работы программы (испольняемого файла).

Наименование программ и файлов могут быть какими угодно, поскольку легко могут быть изменены, однако, их длинна должна быть неизменной. Время и дата изменения этих файлов и программ должны быть полностью идентичны с временем и датой их возникновения на компьютерном устройстве пострадавшей стороны. При этом разделы системного реестра должны содержать указания на размещение и свойства установленных программных файлов.

На компьютерном устройстве злоумышленника образуются файлы и программы, которые являются управляющей частью вредоносной программы, а также:

- откопированные с компьютерного устройства пострадавшей стороны файлы данных и программы, а также «скриншоты» с вышеуказанного компьютерного устройства;
- файлы и папки электронной почты и прикрепленных исполняемых файлов, свойства почтовой программы. В указанных папках могут находиться пароли с компьютерного устройства пострадавших, «логины» для входа в информационные сети, незаконно откопированная информация и др.;
- файлы настроек программ удаленного соединения компьютера с информационной сетью и т.п.;
- отдельные кластеры магнитного носителя информации (винчестера, дискеты), в которых записываются фрагменты исполняемых файлов (программ) и файлов настроек.

Необходимо отметить, что кроме вышеописанных виртуальных следов преступлений, совершаемых с использованием компьютерных технологий, имеют место и традиционные в криминалистике, следы: бумажные документы; следы рук; микрообъекты; идеальные следы и др. Следообразование последних не отличается от ранее хорошо изученного и описанного в научной литературе.

В заключении хотелось бы отметить, что в предмет Криминалистической техники необходимо ввести приемы работы с «виртуальными следами» (поиск, обнаружение, фиксация, исследование). А в уголовно-процессуальном законодательстве необходимо закрепить весь механизм вышеуказанных действий с целью повышения эффективности борьбы с «киберпреступностью».

Библиографический список

1. Номоконов В.А., Тропина Т.Л. Киберпреступность, как новая криминальная угроза // Криминология: вчера, сегодня, завтра. - 2012. - № 24. - С.45-55.
2. Вехов В.Б. Криминалистическое учение о компьютерной информации и средствах ее обработки: автореф. дис. д-ра юрид. наук. - Волгоград, - 2008. - 45 С.
3. Зайцев А.А. Проблемы использования компьютерной техники при раскрытии, расследовании преступлений и доказыванию по уголовным делам // В сборнике: Тактико-методические особенности расследования экономических и иных преступлений. - Казань, - 2018. - С. 138-145.

4. Семенов А.Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации // Сибирский юридический вестник. - 2004. - № 1. - С. 53-55.
5. Краснова Л.Б. Компьютерные объекты в уголовном процессе и криминалистике: автореф. дис. ... канд. юрид. наук. Воронеж, 2005. - 24 с.
6. Зайцев А.А., Смолин А.В. О некоторых элементах криминалистической характеристики киберпреступлений // Криминалистика: вчера, сегодня, завтра. - 2019. - № 3(11). - С. 35-41.
7. Павлюков В.В. Компьютерная разведка, как оперативно-розыскное мероприятие // Вестник Нижегородской академии МВД России. - 2016. - № 4 (36). - С. 236-241.

TRACES OF CYBERCRIME

Zaitsev A.A., Smolin A.V.
Nizhny Novgorod Academy of the Ministry of internal Affairs of the Russian Federation, Nizhny Novgorod
email: alexej.zaitseff2011@yandex.ru

Abstract. The article deals with the mechanism of trace formation of virtual traces of crimes committed with the use of computer technology, types of "virtual traces", and features of their detection. Attention is also paid to some ways of committing cybercrime.

Keywords: investigator, cybercrime, virtual trail, computer equipment, information, software.