УДК 004.9

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ И КОММУНИКАЦИЙ, ИСПОЛЬЗУЕМЫЕ КИБЕРПРЕСТУПНИКАМИ ДЛЯ КОНСПИРАЦИИ СВОЕЙ ДЕЯТЕЛЬНОСТИ

О. А. Слащинин

Следственный комитет Республики Беларусь,
ул. Фрунзе, 19, 220034, г. Минск, Беларусь, a.slashchynin@sledcom.by

Рассмотрены программные, аппаратные и программно-аппаратные средства защиты информации и обеспечения безопасной коммуникации, используемые при организации и совершении киберпреступлений. Факт указанного использования установлен и описан в рамках осуществления предварительного расследования по уголовным делам в сфере информационных технологий. Сами методы защиты информации и коммуникаций описаны лишь через их теоретические аспекты и без упоминания наименований конкретных программных или аппаратных продуктов. В работе упомянуты методы, в отношении которых в настоящее время существуют способы противодействия, применяемые правоохранительными органами в рамках проведения оперативно-розыскных мероприятий и следственных действий.

Ключевые слова: виртуализация; защита информации; информационная безопасность; киберпреступность; обфускация; форензика; шифрование.

Введение. Одной из глобальных проблем современности является киберпреступность как явление и следствие научно-технической революции конца XX – начала XXI веков. С последующим развитием информационных технологий данная проблема не перестанет быть актуальной в связи ростом уровня киберпреступности относительно общего уровня преступности. Причинами роста уровня киберпреступности являются: 1) повышение доступности компьютерной техники; 2) возможность подключения к сети Интернет для всех слоев населения; 3) цифровизация большинства сфер жизнедеятельности общества и государства. Совершение киберпреступления (далее – преступление) предполагает, как правило, удаленное сетевое взаимодействие с потерпевшим или предметом преступления, что вместе с другими элементами конспирации формирует у киберпреступника (далее – преступник) чувство пребывания в условиях анонимности. Исходя из вышеизложенного, преступники совершают противоправные деяния как единолично, так и в составе неустойчивой группы лиц по предварительному сговору, организованной группы или преступной организации (далее – ОПГ). В целях конспирации своей преступной деятельности используют различные правовые (например, подписание участником ОПГ обязательства о неразглашении «коммерческой» тайны), организационные (например, прохождение участником ОПГ полиграфологического исследования, запрет использования личной компьютерной техники (мобильных устройств), а также технические меры защиты информации и коммуникаций. В настоящей работе описаны лишь технические (аппаратные, программные и аппаратно-программные) меры защиты информации и коммуникаций, используемые преступниками для конспирации своей противоправной деятельности.

Основная часть. В настоящее время существует множество методов и отдельных приемов, применяемых преступниками для противодействия компьютерной криминалистике (контр-форензика) и конспирации своей деятельности в киберпространстве. Предлагается поочередно рассмотреть вышеуказанные методы и приемы, начиная от фундаментальных элементов защиты и заканчивая узконаправленными способами противодействия конкурентам (в осуществляемой преступной деятельности) или правоохранительным органам. Перед их рассмотрением стоит отметить, что последние в зависимости от поставленных задач применяются как в комплексе, так и отдельно от всех нижеописанных, а также могут являться элементами единой программной (программно-аппаратной) системы.

1. Шифрование и обфускация. Использование прикладных криптографических инструментов позволяет преобразовывать оригинальные структурированные массивы данных в равномерно распределенную случайную последовательность байтов для их конфиденциальности. Последняя обеспечивается посредством выбора криптографически стойкого алгоритма шифрования, предполагающего вычислительную сложность полного перебора ключа и отсутствие у выбранного алгоритма уязвимостей. При отсутствии вышеуказанных ключей или явной уязвимости криптографического алгоритма практически исключается возможность компрометации скрываемых преступниками массивов данных, независимо от их типа (электронные файлы (далее – файл), области памяти, сетевые пакеты данных и иное).

1.1. Шифрование системы, файловых контейнеров. Для предотвращения возможности получения доступа к программной панели управления компьютерной техники (мобильного устройства) и исследования их накопителей конкурентами или правоохранительными органами преступники шифруют весь накопитель памяти (далее – накопитель) используемого устройства, в том числе его загрузочные разделы с операционной системой (далее – ОС). Помимо системных разделов шифруются внешние накопители (например, USB-флеш-накопители и карты памяти), их логические разделы (тома). Практичным способом шифрования компрометирующей и иной критичной информации является создание файловых криптоконтейнеров, хранящихся внутри общего массива данных физического накопителя или загруженных на удаленные сетевые (облачные) хранилища. Также может использоваться отрицаемое шифрование (контейнер с «двойным дном»), при котором ввод одного ключа предполагает выдачу легитимных некритичных файлов преступника и обеспечение правдоподобного отрицания наличия других скрытых данных, а при вводе другого ключа – выдачу реально скрываемой информации. Стоит упомянуть о возможности настройки шифрования с теми условиями, что при вводе определенного количества неверных ключей или конкретного «ключа самоуничтожения», полезное содержимое накопителя, его логического раздела или файлового криптоконтейнера может быть безвозвратно перезаписано.

1.2. Обфускация сетевого трафика. В целях обхода государственных Интернет-фильтров (далее – фильтр), противодействия глубокой проверки сетевых пакетов данных или для подмены IP-адреса устройства, преступники могут использовать методы, направленные на сокрытие полезных данных указанных пакетов путем их обфускации (запутывания). Существуют следующие основные методы обфускации: 1) шифрование; 2) туннелирование (скрывается факт использования шифрования или иного инструмента противодействия фильтрам); 3) мимикрия (преобразование блокируемых фильтрами полезных данных сетевых пакетов в такие данные, сетевые пакеты которых будут пропускаться через указанные фильтры); 4) рандомизация (случайное преобразование каждого байта полезных данных сетевых пакетов). Применяемые методы обфускации препятствуют корректному исследованию содержания Интернет-сеансов преступников со стороны конкурентов (в случае противоправного перехвата Интернет-трафика) или правоохранительных органов, а также корректному определению IP-адресов устройств, используемых преступниками для доступа к сети Интернет или иным глобальным компьютерным сетям.

1.3. Шифрование передаваемых сообщений (сигналов). Для конфиденциального обмена сообщениями (сигналами) и осуществления аудио-видео вызовов преступники используют различные системы (службы) мгновенного обмена сообщениями, поддерживающие, как правило, открытые и децентрализованные протоколы передачи информации на основе симметричного или ассиметричного сквозного шифрования. В вышеуказанных системах, помимо предустановленных по умолчанию криптографических протоколов сквозного шифрования передаваемых сообщений, преступники используют дополнительное программное обеспечение (далее – ПО), выполняющее на стороне клиента операции ассиметричного шифрования и цифровой подписи обмениваемых сообщений и файлов. Вышеуказанное ПО также используется

преступниками для обеспечения конфиденциальности, аутентификации и проверки целостности сообщений (файлов) обмениваемых посредством служб электронной почты или иных незащищенных каналов связи, но после предварительной сверки открытых ключей шифрования.

1.4. Обфускация ПО. Выполняя свои специфические задачи, преступники могут разрабатывать и использовать собственное, в том числе вредоносное, ПО, а также иные утилиты и скрипты. В целях усложнения декомпиляции и исследования функциональности вышеуказанного ПО со стороны правоохранительных органов или конкурентов применяется запутывание исходного (исполняемого) кода программы посредством различных обфускаторов.

2. Виртуализация и портативность. В случае задержания преступника по месту пребывания последнего может быть обнаружена компьютерная техника (мобильные устройства), содержащая накопители с компрометирующей и иной критичной информацией. В целях предупреждения возможной компрометации преступники организуют и изолируют свои рабочие столы и хранилища с помощью средств виртуализации (эмуляции, контейнеризации), Live-систем или удаленных сетевых (облачных) накопителей.

2.1. Использование удаленных (виртуальных) рабочих столов и хранилищ. Независимо от способа (серверный или облачный) организации удаленных рабочих столов, указанная технология позволяет преступникам получать безопасный доступ к своим файлам и осуществлять противоправную деятельность с относительно любой компьютерной техники (мобильного устройства), имеющей доступ к сети Интернет или иным глобальным компьютерным сетям. Использование изолированной среды удаленного рабочего стола или сетевого (облачного) хранилища позволяет предупредить обнаружение конкурентами или правоохранительными органами компрометирующей и иной критичной информации преступника, в том числе удаленной, при исследовании компьютерной техники-хоста (мобильных устройств) последнего. При такой организации своей деятельности на вышеуказанной технике-хосте правоохранительными органами ничего компрометирующего обнаружено не будет, за исключением факта и адресов подключения к указанным удаленным сетевым ресурсам рабочих столов или хранилищ.

2.2. Виртуальные машины, контейнеры и песочницы. Как указывалось ранее, использование изолированных от хоста сред позволяет предупредить обнаружение правоохранительными органами или конкурентами компрометирующей и иной критичной информации, в том числе удаленной. В данном случае вышеуказанные среды создаются посредством предустановленных на компьютерной технике-хосте гипервизоров, эмуляторов, программных контейнеров или песочниц, в которых уже и выполняется те или иные противоправные действия без относительного оставления цифровых следов на хосте. Также запуск системы или ПО в виртуальной среде предупреждает возможность заражения используемой преступником компьютерной техники-хоста со стороны правоохранительных органов или конкурентов.

2.3. Live-системы (Live-CD/USB). Изолирование своего виртуального рабочего места можно также осуществить с помощью Live-систем, установленных на CD/USB-флеш-накопителях, подключаемых к компьютерной технике-хосту и работающих за счет его процессора, оперативной памяти и иных ресурсов. Вышеуказанные накопители портативны, легко уничтожаются в случае необходимости и, как правило, не логируют действия, запускаемые преступниками в сеансах ОС: ни на самом Live-накопителе, ни на компьютерной технике-хосте.

3. Безопасное удаление данных. При стандартном удалении содержимого накопителей компьютерной техники (мобильных устройств) правоохранительными органами или конкурентами может быть обнаружена остаточная компрометирующая и иная критичная информация преступников. Для предупреждения подобной возможности применяются алгоритмы безопасного удаления компьютерной информации, основанные на программной перезаписи содержимого накопителя случайными данными многочисленными проходами (от 1 до 35 прохо-

дов по методу Гутмана [2]). Это также касается удаления компрометирующих и иных критичных метаданных и скрытых файлов. Данный способ имеет высокую эффективность очистки остаточной информации при отсутствии у преступников возможности систематически размагничивать и менять накопители своих устройств или саму компьютерную технику (мобильные устройства).

4. Стеганография. При выполнении своих специфических задач у преступников может возникнуть необходимость в хранении или передаче текстовой информации или файлов с сокрытием самого факта такого хранения или передачи. Скрываемая информация может содержаться и передаваться через подмену символов, неиспользуемые области, особые свойства или зарезервированные поля текстовых данных, изображений, аудио-видеофайлов и сетевых пакетов данных. Современные стегосистемы позволяют скрыть сам факт наличия стегоконтейнеров и в отличие от шифрования их нельзя достоверно определить посредством измерения уровня энтропии, критерия согласия χ 2 «Хи-квадрат», аппроксимации числа π (Пи) методом Монте-Карло, определения коэффициента автокорреляции, установления величины арифметического среднего или оценки плотности распределения байт [2, С. 232-234].

5. Работа под чужим флагом. При подключении к удаленным сетевым ресурсам преступники изменяют все возможные программные идентификаторы своей компьютерной техники (мобильных устройств), чтобы выдать себя за конкретное лицо, участника определенной социальной группы или другое случайное лицо, никак не связанное с преступником или ОПГ. Программная генерация или изменение уже существующих идентификаторов осуществляется концептуально (согласно выбранной преступником легенды) или случайно. Как правило, это касается тех идентификаторов, которые логируются сетевыми ресурсами или воспринимаются другими лицами, а именно: 1) создание доменного имени сетевого ресурса; 2) генерация адреса электронной почты, в том числе в рамках созданного преступником доменного имени почтового сервера; 3) подмена идентификатора Caller ID абонента вызова или выбор конкретного абонентского номера; 4) изменение IMEI мобильного устройства; 5) генерация User-Agent Интернет-браузера; 6) изменение MAC-адреса сетевого оборудования; 7) установка необходимых для легенды даты и времени (часового пояса) ОС; 8) генерация логина, сетевого имени, пароля, аватара и иных регистрационных данных сетевого ресурса; 9) синтез голоса и (или) изображения (DeepFake) во время аудио-видео вызова или отправки сообщений.

6. Усложнение аутентификации. Для обеспечения безопасности своих файловых контейнеров, учетных записей ПО и сетевых ресурсов преступники, помимо организации менеджеров паролей, используют различные средства усложнения процесса аутентификации. Так, преступниками используются следующие виды, методы и способы аутентификации: 1) генерация надежного случайного пароля или ключа доступа произвольной длины; 2) использование неочевидных ключевых файлов; 3) использование двух-многофакторной аутентификации посредством SMS-сообщений, заранее сформированных или временно сгенерированных аутентификатором кодов, TouchID, FaceID и иных динамических или статических методов биометрической аутентификации, а также иных кодов безопасности; 4) предъявление цифрового сертификата; 5) использование аппаратного USB-токена; 6) использование cookies и привязки к статическому IP-адресу.

7. Использование криптовалют. Для легализации и беспрепятственной транспортировки доходов, полученных преступным путем, осуществления взаимных расчетов между собой или приобретения определенных услуг преступники используют различных цифровые знаки и токены, являющиеся единицей учета операции в информационной системе обмена виртуальными активами. Для функционирования и защиты указанной системы применяется технология блокчейн (англ. blockchain – цепочка из блоков), отдельные особенности которой усложняют процесс установления (деанонимизации) ее пользователей со стороны правоохранительных органов или конкурентов, а именно: 1) распределенный реестр блоков транзакций, пре-

пятствующий единоличному внесению в него изменений, в том числе для блокирования отдельных криптовалютных кошельков, конфискации или ареста конкретных цифровых знаков (токенов); 2) децентрализованная (одноранговая) сеть, основанная на равноправии ее участников (узлов), предполагающем относительную невозможность влияния отдельных субъектов на работу всей системы, а также ее принудительного отключения или блокирования сетевого доступа к ней; 3) использование криптографических методов защиты информации при генерации открытых и приватных ключей криптовалютных кошельков, а также при проверке полномочий участника на совершение действий в системе [3]. Также преступниками в целях дополнительной конфиденциальности могут использовать «анонимные» блокчейны, применяющие следующие криптографические технологии: 1) сокрытие адреса криптокошелька; 2) кольцевая подпись транзакций; 3) автоматический миксер транзакций; 4) доказательство транзакции с нулевым разглашением.

8. Средства антивирусной защиты и межсетевые экраны. Для предотвращения заражения или удаленного несанкционированного подключения со стороны правоохранительных органов или конкурентов к используемой преступниками компьютерной технике (мобильным устройствам) последними применяются ПО для обнаружения компьютерных вирусов, но, как правило, со специфическими базами вирусных сигнатур, а также брандмауэры для контроля и фильтрации всего входящего и исходящего сетевого трафика.

Выводы. В связи с непрерывным эффективным противодействием со стороны правоохранительных органов преступники вынуждены постоянно совершенствовать вышеописанные методы защиты информации и коммуникаций. Упомянутое совершенствование не означает, что преступники самостоятельно проводят исследования и разработку методов защиты информации и коммуникаций, хотя не исключено и подобное. Однако они активно следят за тенденциями и разработками в области информационной безопасности, и при их успешной апробации – перенимают для использования в своей деятельности. От перенятия и использования преступниками наиболее гибких и совершенных методов обеспечения своей информационной безопасности зависят их доход, спокойствие, свобода, а при отдельных обстоятельствах – жизнь. В свою очередь, вышеуказанные методы применимы и в других сферах, не связанных с преступностью, например, правоохранительная деятельность, государственная или частная разведки, а также различные бизнес-проекты.

Библиографические ссылки

1. Gutmann P. Secure Deletion of Data from Magnetic and Solid-State Memory [Электронный ресурс]. URL: www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html (дата обращения: 30.03.2024).

2. Слащинин О. А. Проблема использования энтропии как способа определения данных, представляющих интерес для реализации задач правоохранительных органов // Трансформация механико-математического и IT-образования в условиях цифровизации = Transformation of the mechanical-mathematical and IT-education in the context of digitalization: материалы междунар. науч.-практ. конф., посвящ. 65-летию мех.-мат. фак., Респ. Беларусь, Минск, 26-27 апр. 2023 г. В 2 ч. Ч. 2 / Белорус. гос. ун-т ; редкол.: Н. В. Бровка (гл. ред.) [и др.]. Минск : БГУ, 2023. С. 229-236.

3. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System (2008) / Bitcoin [Электронный ресурс]. URL: bitcoin.org/bitcoin.pdf (дата обращения: 30.03.2024).