УДК 343.9

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КАК СРЕДСТВО СОВЕРШЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

С.А. Лапин, В.В. Поляков
Алтайский государственный университет
г. Барнаул

Статья посвящена анализу программного обеспечения, которое применяется при совершении компьютерных преступлений. Рассмотрены группы программных средств, используемых на разных стадиях преступной деятельности и при различных способах неправомерного удаленного доступа к автоматизированному рабочему месту пользователя. Проведенная классификация вредоносного программного обеспечения способствует повышению эффективности предупреждения и профилактики компьютерной преступности.

Ключевые слова: программное обеспечение, компьютерные преступления, компьютерная информация.

Развитие информационных технологий сопровождается стремительным ростом компьютерной преступности и, что еще более важно, ее качественным изменением. Большинство преступлений в сфере компьютерной информации происходит по каналам удаленной телекоммуникационной связи. Способы их совершения становятся все более высокотехнологичными, содержат нетривиальные технические решения за счет применения как общедоступных компьютерной техники и технологий, так и благодаря применению специально разрабатываемых вредоносных программ. Использование таких ресурсов и возможностей приводит к исключительно высокой латентности компьютерных преступлений, достигающей 99% [1]. Эти обстоятельства требуют тщательного изучения средств и способов, приводящих к росту данного вида преступности.

Средства совершения компьютерных преступлений являются комплексным понятием, включающим в себя компьютерную технику в различных вариантах исполнения (ноутбуки, планшеты, смартфоны и пр.), компьютерные технологии, например, беспроводные Wi-Fi, Bluetooth, 3G, WiMAX, IRDA, LTE и другие, а также программное обеспечение, находящееся в открытом доступе, в закрытом или ограниченном обороте и имеющее различное предназначение [2-4]. В подавляющем большинстве случаев главную роль при совершении компьютерных преступлений занимает именно программное обеспечение, установленное на компьютерах, а не сама по себе компьютерная техника. Другими словами, аппаратные средства по отношению к программным выполняют при совершении компьютерных преступлений обслуживающую роль. Этим определяется важность классификации и анализа программного обеспечения, используемого в преступных целях.

Аппаратные средства, применяемые для негласного съема информации (например, кейлогеры, которые вставляются между разъемом для клавиатуры и самой клавиатурой) действуют в отношении конкретного компьютера и их установка требует отдельных усилий, которые персонифицируют преступника. Кроме того, в этом случае преступникам приходится приобретать специальную технику, которая зачастую является запрещенной. В силу этого неправомерный доступ к компьютерной информации осуществляется обычно удаленным образом, при использовании свободно распространяемой компьютерной техники и специализированного вредоносного программного обеспечения [5, 6]. Это позволяет осуществить атаку одновременно на большое число компьютеров, при этом выявление преступника крайне затруднено. Отметим, что следственными органами сведения о средствах, использованных для совершения преступления, крайне редко бывают получены из заявлений со стороны потерпевших, чаще они поступают из рапортов оперативно-розыскных и других компетентных органов. Эти сведения трудно трансформировать в доказательства, то есть они играют только ориентирующую роль.

Выбор конкретных средств совершения преступления напрямую зависит от объекта посягательства, принятого на нем организационного режима охраны, технических и программно-аппаратных средств защиты информации.

В настоящей статье рассмотрено наиболее распространенное программное обеспечение, которое позволяет совершать преступления в сфере компьютерной информации.

Соответствующие программные средства удобно подразделить на группы: средства, используемые только или в том числе на стадии подготовки к преступлению; применяемые непосредственно при его совершении; используемые при сокрытии следов преступления (при этом сокрытие возможно до, во время и после совершения преступления), а также привлекаемые при противодействии следствию, когда правоохранительным органам стало известно о преступлении [7].

Для неправомерного удаленного доступа к компьютерной информации может быть применено специализированное программное обеспечение, позволяющее осуществлять полное или частичное управление автоматизированным рабочим местом жертвы, либо программное обеспечение, непосредственно не предназначенное для управления автоматизированным рабочим местом, но также обеспечивающее доступ к компьютерной технике (рисунок 1). В программном обеспечении, предназначенном для полного или частичного управления автоматизированным рабочим местом с доступом к хранимой на нем компьютерной информацией, нужно выделить две основные группы: вредоносное программное обеспечение и разрешенное программное обеспечение. Отметим, что данное деление достаточно условное, так как признание программного обеспечения вредоносным является юридическим вопросом, окончательное решение принимается только судом [8]. Тем не менее, отличительной особенностью вредоносного программного обеспечения является именно несанкционированный доступ к управлению автоматизированным рабочим местом, кража различного рода компьютерной информации, а также использование аппаратных или сетевых ресурсов автоматизированного рабочего места. Рассмотрим программы и технологии, которые могут использоваться в этих целях.

На стадии подготовки к совершению преступления могут применяться специальные программы - шпионы, которые скрыто от пользователя передают преступнику информацию о компьютере жертвы, например, конфигурацию и данные о конкретном программном обеспечении, средствах используемой защиты информации и т.п. Часто такой информацией бывают cookie браузера, сохраненные и вводимые пользователем пароли, сертификаты, скриншоты экрана, данные о наличие e-token и т.п.

Центральным элементом способа совершения преступления обычно выступают средства, предоставляющие возможность управлять автоматизированным рабочим местом пользователя на основе сетевых протоколов RDP (Remote Desktop Protocol) или VNC (Virtual Network Computing). За счет их использования преступник может удаленно работать с автоматизированным рабочим местом жертвы. При этом вредоносное программное обеспечение, в основе которого лежит протокол RDP, работает по принципу анонимности таким образом, что пользователь не видит на экране своего монитора действия, который в данный момент выполняются с его компьютером.

Еще одной разновидностью вредоносного программного обеспечения являются эксплойты. Они представляют собой один из основных методов заражения автоматизированного рабочего места. Под эксплойтом понимается программный код или его фрагмент, который через ошибки в каком-либо программном обеспечении, работающем в данный момент времени на атакуемом компьютере, приводит к выполнению этим программным обеспечением действий, непредусмотренных его разработчиками. Как правило, эксплойты применяются для повышения привилегий (прав доступа) в операционной системе либо для первого запуска какой-либо вредоносной программы, которая в дальнейшем будет запускаться уже автоматически.

Для высокотехнологичных способов совершения компьютерных преступлений характерно использование программного обеспечения, специально написанного преступником или по его заказу сообщниками из числа преступной группы, а также посторонними специалистами, которые могут относиться безразлично к тому, в каких преступлениях оно будет применено. Здесь речь идет, как правило, о так называемых шеллах (shell), которые при запуске на компьютере позволяют злоумышленнику выполнять достаточно ограниченный круг команд по управлению автоматизированным рабочим местом. Такой командой может быть, например, загрузка файла на зараженный компьютер или загруз-

ка файл из зараженного автоматизированного рабочего места на компьютер преступника, выполнение какого-либо действия командной оболочкой операционной системы и т.д. Данное программное обеспечение работает скрытно от пользователя и запускается вместе с запуском операционной системы по протоколам RDP или VNC. Необходимо отметить, что существует вредоносное программное обеспечение, которое может включать в себя различную функциональность. К этому виду программ можно отнести программное обеспечение, предназначенное для кражи денежных средств с банковских счетов пользователей (как, например, SpyEye, Zeus, Carberp).

Неправомерный доступ к автоматизированному рабочему месту может быть осуществлен злоумышленником и с помощью легитимного программного обеспечения, предоставляющего управление компьютером. Такие программы могут входить в состав операционной системы или могут быть установлены самими пользователями в качестве дополнительного программного обеспечен. Сейчас существуют множество подобного рода программ: удаленный рабочий стол в ОС Windows, VNC сервер, TeamViewer, Radmin и другие. Преступник может эксплуатировать данное программное обеспечение, подобрав или подсмотрев к нему пароль, либо запустить его через вредоносную программу.

В ряде случаев неправомерный доступ к компьютерной информации может быть осуществлен без использования программного обеспечения, позволяющего каким-либо образом управлять автоматизированным рабочим местом. В качестве примера можно привести атаки на почтовые аккаунты пользователей, находящихся на популярных почтовых сервисах, таких как gmail.com, mail.ru, qip.ru, aol.com и т.п. При создании пользователем подобного рода аккаунтов ему предлагается ввести пароль и ответы на ключевые вопросы для обеспечения защиты, по которым в случае, если пользователь забыл свой пароль, его можно было бы восстановить. При этом злоумышленник может удаленно подобрать пароль или ответы на ключевые вопросы для смены пароля, что обеспечит ему беспрепятственный неправомерный доступ к компьютерной информации, хранящейся в почтовом аккаунте.

Приведенная классификация программного обеспечения, используемого при совершении компьютерных преступлений, может быть использована для повышения эффективности противодействия компьютерной преступности и в целях ее профилактики.

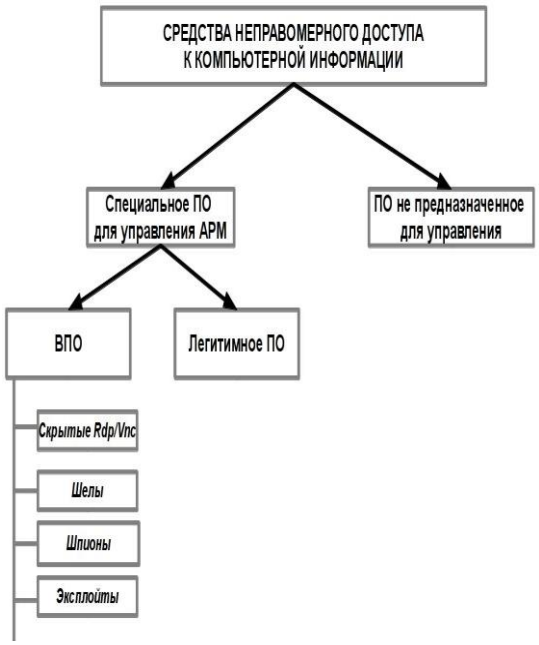

Рисунок 1 – Классификация программного обеспечения, используемого при совершении компьютерных преступлений

Публикация подготовлена в рамках поддержанного РГНФ научного проекта №16-33-01160.

СПИСОК ЛИТЕРАТУРЫ

1. Степанов-Егиянц В.Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями // Российский следователь. – 2012. - № 24. - С. 43-46.
2. Веденеев В.С., Бычков И.В. Средства поиска инсайдеров в корпоративных информационных системах // Безопасность информационных технологий. 2014. №1. С. 9-13.
3. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества // М.: ООО Изд-во «Юрлитинформ», 2002. 496 с.
4. Язов Ю.К., Сердечный А.Л., Шаров И.А. Методический подход к оцениванию эффективности ложных информационных систем // Вопросы кибербезопасности. 2014. 1 (2). С. 55-60.
5. Гавло В.К., Поляков В.В. Следовая картина и ее значение для расследования преступлений, связанных с неправомерным удаленным доступом к компьютерной информации // Российский юридический журнал. 2007. №5 (57). С. 146-152.
6. Поляков В.В. Криминалистическая структура мер предупреждения компьютерных преступлений // Библиотека криминалиста : научный журнал. 2013. №5 (10). С. 287 - 291.

7. Осипенко А.Л. Оперативно-розыскная деятельность в киберпространстве: ответы на новые вызовы // Научный вестник Омской академии МВД России. 2010. № 2 (37). С. 38-43.
8. Корухов Ю.Г., Парфентьев А.М. Необходимость совершенствования правовой регламентации применения научных и технических средств // Информационный бюллетень академии управления МВД России. 2000. № 12. С. 8–13.

Лапин Сергей Александрович – аспирант кафедры прикладной физики, электроники и информационной безопасности, тел.: (3852) 364-809, e-mail: lapinsa567@gmail.com;
Поляков Виталий Викторович – к.ю.н., доцент кафедры уголовного процесса и криминалистики, тел.: (3852) 366-492, e-mail: agupolyakov@gmail.com.