ISSN 2500-4255

УДК 343.98
DOI 10.17150/2500-4255.2020.14(5).699-709

КОНЦЕПЦИЯ ВРЕДОНОСНЫХ ПРОГРАММ КАК СПОСОБОВ СОВЕРШЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ: КЛАССИФИКАЦИИ И ТЕХНОЛОГИИ ПРОТИВОПРАВНОГО ИСПОЛЬЗОВАНИЯ

Е.Р. Россинская[1], И.А. Рядовский[2]
[1] Московский государственный юридический университет им. О.Е. Кутафина (МГЮА), г. Москва, Российская Федерация
[2] Акционерное общество «Лаборатория Касперского», г. Москва, Российская Федерация

Информация о статье

Дата поступления
17 марта 2020 г.

Дата принятия в печать
30 октября 2020 г.

Дата онлайн-размещения
20 ноября 2020 г.

Ключевые слова
Компьютерные преступления; вредоносная программа; несанкционированный доступ; программа-вирус; программа-червь; троянская программа; программа-шифровальщик; «бестелесная» технология; компьютерная атака на отказ в обслуживании; бот-сеть; фишинговое письмо

Финансирование
Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16003

Аннотация. С позиций учения о способах совершения компьютерных преступлений/правонарушений как одной из составляющих теории информационно-компьютерного обеспечения криминалистической деятельности рассмотрены проблемы, связанные с вредоносными компьютерными программами. Отмечено, что в основе большинства способов совершения компьютерных преступлений лежит несанкционированный доступ к компьютерным средствам и системам, осуществляемый с помощью вредоносных программ, которые фактически выступают в качестве орудий совершения преступления. Даны классификации вредоносных программ по различным основаниям: с позиции уголовного права и криминологии; с информационно-технологической позиции; с позиции учения о способах совершения компьютерных преступлений/правонарушений. Рассмотрены разные основания классификации вредоносных программ. Общая классификация, широко применяемая разработчиками антивирусного программного обеспечения, включает программы-вирусы, программы-черви и троянские программы. Указано, что в современных условиях массовой цифровизации выделять в качестве основного признака троянской программы маскировку под легитимный файл нецелесообразно. Напротив, преступники стараются максимально скрыть от пользователя загрузку, установку и работу не имеющей возможности саморазмножения вредоносной программы. Основным способом распространения троянских программ является массовая рассылка сообщений на электронную почту, содержащих вложения, маскирующиеся под полезный для пользователя документ. Классификация вредоносных программ по способу и методу распространения — вирусы, черви и троянские программы — в настоящее время сохраняется только в силу традиции и часто не отражает сути процесса. Другая классификация вредоносных программ — на автоматические, полуавтоматические и неавтоматические — основана на возможности их автономной работы. В настоящее время вредоносные программы, функциональность которых охватывала бы только конкретный вид действий, практически не встречаются, большинство сочетает целый набор видов деятельности, реализуемый путем использования модульной архитектуры, что предоставляет преступникам широкие возможности для манипулирования информацией. Описаны и проиллюстрированы с помощью примеров основные механизмы действия вредоносных программ. Особое внимание уделено вредоносным программам-шифровальщикам, действующим с применением стойких криптографических алгоритмов, — программам-вымогателям, когда за восстановление данных преступники требуют выкуп. За совершение подобных хищений уголовная ответственность не предусмотрена. Обозначены проблемы, связанные с возможностью появления новых вредоносных программ, поражающих облачные ресурсы.

THE CONCEPT OF MALWARE AS A MEANS OF COMMITTING COMPUTER CRIMES: CLASSIFICATION AND METHODS OF ILLEGAL USE

Elena R. Rossinskaya[1], Igor A. Ryadovskiy[2]
[1] Kutafin Moscow State Law University (MSAL), Moscow, the Russian Federation
[2] Kaspersky Lab Ltd., Moscow, the Russian Federation

Article info

Received
2020 March 17

Abstract. The authors analyze problems connected with malware from the standpoint of the doctrine of the methods of computer crimes/offenses as one of the components of the theory of information-computer support of criminalistic work. Most methods of computer crimes are based on the unauthorized access to computer

ISSN 2500-4255

Accepted
2020 October 30
Available online
2020 November 20

Keywords
Computer crimes; malware; unauthorized access; virus-program; worm-program; trojan-program; ransomware; «fileless» technology; distributed denial of service attack; botnet; phishing email

Acknowledgements
The study was financially supported by the Russian Foundation for Basic Research within Research Project № 18-29-16003

facilities and systems gained through malware that, in fact, acts as a weapon of crime. The authors present a classification of malware based on different parameters: from the standpoint of criminal law and criminology; the standpoint of information technology; the standpoint of the doctrine of computer crimes/offenses. Various grounds for the classification of malware are examined. A general classification, widely used by the developers of antiviral software, includes virus-programs, worm-programs and trojan-programs. In the modern situation of massive digitization, it is not practical to regard masquerading as a legitimate file as a dominant feature of trojan software. On the contrary, criminals try hard to hide from the user the downloading, installation and activity of malware that cannot self-propagate. The key method of propagating trojan programs is sending mass emails with attachments masquerading as useful content. The classification of malware by the way and method of propagation — viruses, worms and trojan programs — is only currently used due to traditions and does not reflect the essence of the process. A different classification of malware into autonomous, semi-autonomous and non-autonomous programs is based on the possibility of their autonomous functioning. At present there is practically no malware whose functions include only one specific type of actions, most of it contains a combination of various types of actions implemented through module architecture, which offers criminals wide opportunities for manipulating information. The key mechanisms of malware's work are described and illustrated through examples. Special attention is paid to harmful encryption software working through stable cryptographic algorithms — ransomware, when criminals demand ransom for restoring data. There is no criminal liability for such theft. The authors outline the problems connected with the possibility of the appearance of new malware that would affect cloud resources.

В настоящее время подавляющее число компьютерных преступлений, и в первую очередь связанных с несанкционированным доступом к компьютерным средствам и системам, осуществляется с помощью вредоносных программ, которые значительно усиливают возможности преступников и в этом плане могут рассматриваться в качестве орудий совершения преступления. Понятие «компьютерные преступления» употребляется нами не в уголовно-правовом, а в криминалистическом аспекте, поскольку связано не с квалификацией, а со способами совершения преступлений, которые обладают общей родовой криминалистической характеристикой и, соответственно, во многом общей родовой методикой их раскрытия и расследования [1, с. 440–442].

Вместе с тем сам термин «вредоносная программа», с одной стороны, уже устоялся, но, с другой стороны, это понятие выступает как собирательное. Рассмотрим дефиницию понятия «вредоносная программа» с позиций учения о способах совершения компьютерных преступлений/правонарушений как одной из составляющих теории информационно-компьютерного обеспечения криминалистической деятельности [2]. Ранее мы отмечали, что способы совершения компьютерных преступлений обычно являются полноструктурными (т.е. включают все три элемента: подготовку, совершение и сокрытие), причем подготовка к преступлению зачастую включает сразу и действия по его сокрытию [3]. Чтобы дать строгое определение, необходимо вычленить объективные свойства компьютерной программы, характеризующие ее как вредоносную.

С уголовно-правовой точки зрения определение вредоносной программы содержится в диспозиции ст. 273 УК РФ, согласно которой под таковой понимается компьютерная программа либо иная компьютерная информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации[1].

Признаки состава данного преступления, по существу, можно рассматривать как признаки, позволяющие признать конкретную компьютерную программу вредоносной, но только с правовой точки зрения, так как установление прямого умысла на этапе разработки вредоносной программы, а именно доподлинное и безусловное осознание предназначения создаваемой программы — «заведомо предназначенная», является исключительной прерогативой следователя и суда.

[1] Уголовный кодекс Российской Федерации [Электронный ресурс] : федер. закон от 13 июня 1996 г. № 63-ФЗ : (ред. от 27 дек. 2019 г.) // СПС «КонсультантПлюс».

Иначе трактуют этот термин компании, занимающиеся разработкой программного обеспечения (ПО) и созданием средств защиты информации.

Необходимо отметить, что в англоязычной терминологии используется понятие malware, образованное от слияния двух слов: malicious — злонамеренный и software — программное обеспечение. Компания Microsoft под этим термином понимает вредоносные приложения и программный код, которые могут привести к повреждению и нарушению нормальной работы устройств[2]. Такое определение с криминалистической точки зрения нельзя признать полным, отражающим его сущность.

Более широко это понятие раскрывается в электронной энциклопедии «Лаборатории Касперского», согласно которой вредоносные программы создаются специально для не санкционированного пользователем уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютеров или компьютерных сетей[3].

Сходным образом раскрывает этот термин Национальный институт стандартов и технологий США (NIST), определяя под вредоносным ПО «программное обеспечение или встроенное микропрограммное обеспечение, предназначенные для выполнения несанкционированного процесса, который может оказать неблагоприятное влияние на конфиденциальность, целостность или доступность информационной системы»[4].

На «не санкционированную пользователем реализацию своего назначения» вредоносной программой как на ее ключевой признак обращали внимание еще авторы одного из первых комментариев к ст. 273 УК РФ: «Вредоносность или полезность соответствующих программ для ЭВМ определяется не в зависимости от их назначения, способности уничтожать, блокировать, модифицировать, копировать информацию (это — вполне типичные функции абсолютно легальных программ), а в связи с тем, предполагает ли их действие, во-первых, предварительное уведомление собственника компьютерной информации или другого добросовестного пользователя о характере действия программы, а во-вторых, получение его согласия (санкции) на реализацию программой своего назначения. Нарушение одного из этих требований делает программу для ЭВМ вредоносной» [4, с. 419].

С изложенным мнением трудно не согласиться. Действительно, любая компьютерная программа в процессе своей работы записывает новые и стирает старые данные в оперативной памяти и на подключенных дисках, модифицирует их, согласно заложенному в нее алгоритму может блокировать либо копировать определенную информацию. Однако и эта трактовка вызывает вопросы. Указанные признаки не являются достаточными для признания программы вредоносной, поскольку такая ее функциональность может быть следствием ошибки в разработке либо осознанно реализованной, но по какой-то причине не задекларированной ее создателями. При таких обстоятельствах еще один признак можно рассматривать как необходимый для того, чтобы назвать ПО вредоносным, — субъективное восприятие потерпевшим угрозы от компьютерной программы. Очевидно, что даже при наступлении неких негативных последствий в результате работы известных легальных программ вследствие того, что разработчики ПО не уведомили пользователя о характере действия программ либо не получили разрешения на реализацию программами незадекларированной функциональности, эти факты не могут сами по себе являться основанием для признания ПО вредоносным. Проиллюстрируем такие ситуации несколькими примерами.

В 2017 г. компания Microsoft, разъясняя причины возникших проблем в работе антивирусных программ, установленных пользователем на компьютеры под управлением ОС Windows 10, признала факты кратковременного отключения стороннего антивирусного ПО в связи с обновлением операционной системы [5].

В другом случае проблемы возникли осенью 2019 г. у пользователей компьютеров Mac Pro компании Apple под управлением операционной системы macOS версий 10.9–10.14 Mojave, которые в какой-то момент перестали загружаться. Как выяснилось позже, причиной такого сбоя явилось не заражение компьютеров вредоносной программой, а ошибка разработчиков,

[2] Общие сведения о вредоносных и других угрозах. URL: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/intelligence/understanding-malware.

[3] Энциклопедия «Лаборатории Касперского». Классификация детектируемых объектов. Вредоносные программы. URL: https://encyclopedia.kaspersky.ru/knowledge/malicious-programs.

[4] NIST Special Publication 800-53. Revision 4. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

ISSN 2500-4255

приводящая к некорректному обновлению ПО Google Chrome для Mac. Mac перестали загружаться из-за обновления Google Chrome [6].

Более того, Будапештской конвенцией о киберпреступности особо предусмотрено, что статья о криминализации действий по созданию, распространению и использованию компьютерных программ для совершения упомянутых в первом подразделе Конвенции правонарушений не должна толковаться как устанавливающая уголовную ответственность в тех случаях, когда данные действия не связаны с намерением совершать правонарушения, а, например, осуществлены в связи с разрешенным испытанием или защитой компьютерной системы. В этой связи необходимо отметить, что непосредственно термин «вредоносная программа» в Конвенции не упоминается. Но авторами данного международного правового акта предлагается странам-участницам предусмотреть в национальных законодательствах уголовную ответственность за создание, распространение в различных формах, приобретение и использование компьютерных программ, разработанных или адаптированных для совершения деяний, предусмотренных статьями первого подраздела Конвенции «Правонарушения, связанные с использованием компьютерных средств», в который включены: неправомерный доступ к компьютерной системе или ее части; неправомерный перехват данных, передаваемых в компьютерную систему, из нее или внутри такой системы; умышленное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных; неправомерное воздействие на функционирование компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных[5].

Сходной и даже более широкой трактовки понятия «вредоносная программа» придерживаются и представители отечественной науки уголовного права и криминологии. Так, Е.А. Русскевич на основе анализа признаков вредоносности компьютерного ПО в свете доктрины уголовного права приходит к выводу, что под вредоносной следует понимать компьютерную программу, созданную (в том числе путем модификации легальной программы) для осуществления противоправной деятельности [7, с. 212].

Действительно, стремительная цифровизация практически всех сторон человеческой жизнедеятельности приводит к появлению новых угроз современному обществу. Это выражается и в том, что большинство противоправных посягательств, предусмотренных уголовным законом, а не только преступления, изложенные в гл. 28 УК РФ, могут быть совершены и совершаются с применением компьютерных средств и систем [8, с. 110]. Очевидно, что возможность использования при их подготовке, совершении и сокрытии вредоносных программ не является исключением. При таких обстоятельствах расширенное толкование определения вредоносности компьютерных программ представляется вполне оправданным.

Что касается технико-технологической стороны вопроса, то можно выделить следующие объективные свойства, которые позволяют рассматривать такие программы как обладающие признаками вредоносности:

– наличие функциональных возможностей уничтожения, блокирования, модификации, копирования пользовательской информации и нейтрализации средств защиты компьютерной информации;

– инсталляция без явного одобрения пользователем;

– скрытый либо замаскированный от пользователя режим работы;

– проведение операций с информацией, не санкционированных пользователем явно.

В качестве орудия совершения преступления может быть использована подвергнутая модификации, т.е. адаптированная, легальная программа, основная функциональность которой предоставляет преступникам возможность достижения своих целей. Большинство легальных программ, используемых в противоправной деятельности, предназначено для удаленного несанкционированного доступа к компьютеру, управления системой и ее администрирования. Для своих целей преступники модифицируют их, скрывая от пользователя явно отображаемые на дисплее уведомления и иные признаки удаленного подключения.

Один из таких способов модификации реализуется с помощью технологии DLL Hijacking[6], эксплуатирующей особенности функционирования операционной системы Windows. При

[5] Convention on Cybercrime. Budapest, 2001, 23 November. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

[6] The MITRE Corporation. CWE-427: Uncontrolled Search Path Element. URL: https://cwe.mitre.org/data/definitions/427.html.

запуске программа вместо легального библиотечного файла (dll-библиотеки) загружает вредоносный, который обеспечивает скрытый от пользователя режим работы программы. Такой результат достигается помещением в одну папку с основным файлом программы вредоносной библиотеки.

Таким образом преступник с минимальными затратами получает мощный инструмент для достижения своих целей, при этом инсталлированная на компьютер программа вполне легитимная, а вредоносным является лишь один библиотечный файл, который при запуске программы дополняет ее не предусмотренными разработчиками свойствами.

Вследствие большого разнообразия вредоносных программ для их классификации используют различные основания. Самая общая классификация, широко применяемая в настоящее время разработчиками антивирусного ПО, выделяет из класса вредоносных программ (Malware) следующие подклассы: программы-вирусы (Virus), программы-черви (Worm) и троянские программы (Trojan)[7].

Данная классификация вредоносных программ воспринята и апробирована судебно-экспертным сообществом, что нашло отражение в национальном стандарте ГОСТ Р 57429-2017 «Судебная компьютерно-техническая экспертиза. Термины и определения», разработанном Российским федеральным центром судебной экспертизы при Министерстве юстиции Российской Федерации совместно с Экспертно-криминалистическим центром Министерства внутренних дел Российской Федерации, Московским государственным юридическим университетом им. О.Е. Кутафина (МГЮА) и Следственным комитетом Российской Федерации[8].

В указанном документе даны следующие определения, рекомендуемые в качестве справочных данных, отражающих систему понятий судебной компьютерно-технической экспертизы:

– компьютерный вирус — программа, обладающая способностью к самораспространению по локальным ресурсам средства вычислительной техники, не использующая сетевых сервисов;

– червь — программа, обладающая способностью к самораспространению в компьютерных сетях через сетевые ресурсы;

– троянская программа — программа, не обладающая возможностью самораспространения, маскирующаяся под легитимный файл.

Полагаем, следует уточнить, что, по мнению авторов, в настоящее время выделять в качестве основного признака троянской программы маскировку под легитимный файл уже не является целесообразным. Действительно, изначально под троянской программой понималась разновидность вредоносной программы, которая устанавливалась в компьютерную систему под видом легального ПО и работала, маскируясь под него. Надо отметить, что и зарубежные исследователи продолжают использовать устоявшуюся терминологию, относя к одному из основных видов вредоносных программ тип Trojan horse (с англ. «троянский конь»), очевидно подразумевая под этим названием наличие скрытых деструктивных функциональных возможностей, замаскированных под некую легитимную программу, которую пользователь по собственной воле устанавливает в своей компьютерной системе, не подозревая об ее истинном предназначении [9, p. 229].

Однако ситуация изменилась, и сейчас преступники, напротив, пытаются максимально скрыть от пользователя загрузку, установку и работу не имеющей возможности саморазмножения вредоносной программы, используя для этого различные способы и средства. Даже названия вредоносных файлов часто носят случайный характер и не имеют какого-либо сходства с именами легитимных файлов.

С точки зрения смысловой нагрузки данного термина следует заметить, что в настоящее время основным способом распространения троянских программ является массовая рассылка сообщений на электронную почту, содержащих вложения, маскирующиеся под полезный для пользователя документ, — так называемых фишинговых писем (от англ. fish — ловить рыбу). Использование этого термина подразумевает, что такое письмо содержит некое нежелательное вложение — «крючок», на который попадается жертва. При попытке открытия подобного вложения в систему загружается и устанавливается троянская программа [10]. Другой способ распространения троянских программ посредством рассылки фишинговых писем реализуется не через вложение, а через интернет-ссылку,

[7] Энциклопедия «Лаборатории Касперского». Классификация детектируемых объектов. Вредоносные программы.

[8] ГОСТ Р 57429-2017. Судебная компьютерно-техническая экспертиза. Термины и определения : утв. и введен в действие 28 марта 2017 г. URL: http://docs.cntd.ru/document/1200144960.

при переходе по которой пользователь направляется на сайт, содержащий наборы программ-эксплойтов, пытающихся найти уязвимые места в безопасности его компьютерной системы и через них загрузить вредоносную программу [11].

Данный способ распространения вредоносного ПО на протяжении нескольких лет остается настолько востребованным, что исследователи виктимизации высокотехнологичных преступлений, наряду с традиционными методами их профилактики рассматривая взаимосвязь «пользователь — компьютер», настаивают на применении технических мер для побуждения пользователей отказаться от необдуманных действий по открытию нежелательных вложений либо от перехода по вредоносным ссылкам, прикрепленным к сообщениям на электронную почту [12].

Также смысл названия «троянские» этого типа вредоносных программ прослеживается в способе сокрытия их функционирования в системе, когда вредоносный код внедряется в адресное пространство работающей легальной программы, например в один из системных процессов, в результате чего все запросы троянской программы представляются как легитимно сгенерированные. Но все же стоит признать, что название этого подкласса вредоносных программ в настоящее время является символическим, сохраненным в силу сложившейся традиции разделения их на три группы по способу и методу распространения: вирусы, черви и троянские программы.

Другая классификация вредоносных программ учитывает такую их функциональную особенность, как возможность автономной работы. По этому основанию выделяют автоматические, полуавтоматические и неавтоматические программы [13, с. 86–87].

Автоматические вредоносные программы не нуждаются во внешнем управлении, заложенные в них функциональные возможности реализуются в автономном режиме. При необходимости передать информацию с зараженного компьютера на удаленный сервер программа самостоятельно инициирует соединение [14]. Например, программа-шифровальщик (Trojan-Ransom) после кодирования пользовательских данных инициирует сетевое соединение с удаленным сервером и передает на него информацию, содержащую идентификатор зараженного компьютера, для последующего восстановления пользовательских данных в случае выплаты денежных средств.

Полуавтоматические программы также способны работать автономно. Реализуя свое предназначение, они инициируют соединение зараженного компьютера с удаленным сервером для передачи информации, но при этом они имеют возможность получать с сервера управления команды и выполнять их. К полуавтоматическим относятся практически все троянские программы, предназначенные для хищения в электронных платежных системах (Trojan-Banker). Например, попав в систему, такие программы самостоятельно сканируют пользовательскую информацию, находят следы использования программ-клиентов дистанционного банковского обслуживания, платежные документы, учетные записи и пароли и т.п. и передают собранную информацию на сервер управления. Но при этом они обладают возможностью получения от сервера внешних команд на загрузку дополнительных программных модулей либо на совершение несанкционированной финансовой операции.

Вредоносные программы, работающие в ручном режиме (неавтоматические), предназначены для управления с помощью внешних команд. Такими программами могут быть троянские программы для удаленного управления компьютером (Trojan-Backdoor) либо программы, предназначенные для управления диспенсером банкомата с использованием штатной клавиатуры (пин-пада).

Статистика свидетельствует, что использование вирусов и червей в настоящее время незначительно, хотя в определенных случаях для распространения некоторых видов вредоносных программ было зафиксировано весьма эффективное применение возможностей их саморазмножения в крупных корпоративных сетях. Так, в мае 2017 г. была осуществлена одна из самых масштабных компьютерных атак, затронувшая пользователей по всему миру, в ходе которой распространялась программа-шифровальщик WannaCry[9].

Возможно, эффективное применение такого способа распространения объясняется тем, что использовался эксплойт EternalBlue, похищенный в Агентстве национальной безопасности США [15], а настолько массовые случаи заражения были связаны именно со способом распространения. После успешного проникно-

[9] Программа WannaCry взяла в заложники компьютеры по всему миру. Обобщение // Interfax.ru. 2017. 13 мая. URL: https://www.interfax.ru/world/562164.

вения хотя бы на один компьютер, подключенный к локальной сети, шифровальщик WannaCry распространялся по сети на другие устройства как червь (Worm).

Тем не менее, как подтверждают статистические данные, наибольшую долю существующих ныне вредоносных программ образует подкласс троянских программ, которые представляют собой комплекс вредоносного ПО, состоящий из клиентской части — управляющей и серверной части — программы-бота. Совокупность зараженных конкретным образцом троянской программы компьютеров, управляемых из одного центра, называют бот-сетью. На клиентской части размещен центр управления бот-сетью — сайт (веб-панель), являющийся элементом комплекса вредоносного ПО, предназначенный для управления зараженными компьютерами, а также для накопления, систематизации и анализа переданной с них информации. В иных ситуациях роли в связке «клиент — сервер» могут поменяться, тогда компьютер-бот, отправляя запросы центру управления, выступает в качестве клиентской части.

Основным признаком, который служит для дифференцирования троянских программ, является вид действия (поведение), которое они выполняют на компьютере[10]. Наиболее распространенные в настоящее время виды троянских программ наделены следующими видами действия:

– программа-загрузчик (Trojan-Downloader, Trojan-Dropper) производит загрузку и установку на компьютер других вредоносных программ и их новых версий;

– программа-шпион (Trojan-Spy) осуществляет ведение электронного шпионажа за пользователем, в том числе перехват вводимых с клавиатуры данных, изображений с экрана, списка активных приложений;

– программа-банкер (Trojan-Banker) нацелена на кражу пользовательской информации, относящейся к банковским счетам, системам электронных денег и пластиковым картам;

– программа-шифровальщик (Trojan-Ransom) модифицирует пользовательские данные на компьютере либо блокирует работу компьютера с целью получения выкупа за восстановление доступа к информации;

– программа для удаленного управления (Trojan-Backdoor) предназначена для скрытого удаленного управления компьютером и полного доступа к пользовательской информации;

– программа для эксплуатации программных уязвимостей (exploit) скрыто от пользователя эксплуатирует уязвимости ПО.

Что касается такого вида программ, как эксплойт (exploit), следует уточнить, что помимо программ под этим термином понимается определенный набор данных, который обрабатывается легальной программой, установленной на компьютере пользователя, с не предусмотренным разработчиком этого ПО результатом, приводящим к компрометации системы.

В настоящее время вредоносные программы, функциональность которых охватывала бы только конкретный вид действий, например поиск платежной информации либо перехват вводимых пользователем паролей, практически не встречаются. Большинство современных троянских программ сочетает в себе целый набор видов деятельности, что предоставляет преступникам большие возможности для манипулирования пользовательской информацией. Такая широкая функциональность реализуется посредством использования модульной архитектуры. Каждый дополнительный модуль отвечает за конкретный вид действия, но на зараженном компьютере может работать только во взаимодействии с главным модулем — ядром.

Например, функциональность программы-банкера, определяемой антивирусным ПО «Лаборатории Касперского» с именем Trojan-Banker.Win32.RTM [16], значительно расширяется за счет загрузки дополнительных модулей непосредственно в оперативную память, без сохранения на жестком диске. Но такая особенность их работы применима не только к отдельным модулям. Программы, функционирующие в оперативной памяти компьютера и не сохраняющиеся на энергонезависимые запоминающие устройства, именуют «бестелесными». Этот способ используется для сокрытия вредоносного кода от антивирусного ПО [17].

Собранную основным модулем информацию о компьютерной системе пользователя троянская программа отправляет на управляющий сервер, где она обрабатывается по заданным правилам автоматически либо в ручном режиме оператором центра управления бот-сетью. По результатам анализа собранной основным модулем информации о системе центр управле-

[10] Энциклопедия «Лаборатории Касперского». Классификация детектируемых объектов. Вредоносные программы. Троянские программы. URL: https://encyclopedia.kaspersky.ru/knowledge/trojans.

ния отдает команду на загрузку на компьютер дополнительных модулей, необходимых для реализации преступного умысла. Перечень дополнительных модулей определяется на основе анализа следующей информации:

– версия операционной системы;

– наличие антивирусного ПО и иных средств защиты;

– наличие определенного ПО;

– иные сведения, как, например, аппаратные характеристики, наличие административных привилегий учетной записи и т.п.

Такой подход на определенном этапе развития киберпреступности привел к существенному расширению функциональных возможностей вредоносного ПО, позволяющих эффективно атаковать не только компьютеры физических лиц, но и крупные корпоративные сети. Примерно с 2014 г. регулярные компьютерные атаки, нацеленные на хищение денежных средств либо кражу конфиденциальной информации, стали совершаться в крупных компаниях и учреждениях [18], что существенно увеличило преступные доходы в этой сфере и, как следствие, должно было привести к вовлечению новых участников в преступную деятельность в сфере компьютерной информации.

Еще одна проблема, которая требует своего решения, — отсутствие противодействия ряду правонарушений, совершаемых с использованием определенного вредоносного ПО, в связи с тем, что эти правонарушения находятся за пределами уголовно-правового регулирования. Остановимся предметнее на конкретных видах компьютерных атак для иллюстрации этого тезиса.

Одной из наиболее значительных угроз в сфере компьютерной информации на протяжении последних лет остается распространение вредоносных программ-шифровальщиков, или, как еще их называют, Ransomware (от слияния слов ransom — выкуп и software — программное обеспечение). Задолго до получившей международный резонанс кампании по распространению шифровальщика WannaCry этот вид вредоносного ПО стал одной из самых массовых и разрушительных угроз, с которыми сталкиваются пользователи Интернета [19]. Как уже говорилось выше, данные программы предназначены для несанкционированной модификации пользовательских данных в компьютерных системах, в большинстве случаев — с применением стойких криптографических алгоритмов, что делает невозможной самостоятельную расшифровку модифицированной злоумышленниками информации. За восстановление данных преступники требуют выкуп, причем вымогаемые суммы, как правило, соответствуют крупному и особо крупному размеру, указанному в статьях, предусматривающих ответственность за совершение хищений, либо значительно превышают его. Поэтому такой вид троянских программ называют еще программами-вымогателями.

Очевидно, что объектом рассматриваемого деяния, помимо отношений в сфере безопасного обращения компьютерной информации, ее обработки, передачи и хранения, выступают общественные отношения собственности. Однако в соответствии с действующим законодательством ответственность за вымогательство наступает лишь в случае, если противоправные требования предъявляются под угрозой применения насилия либо уничтожения или повреждения чужого имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких. Несмотря на то что в современную высокотехнологичную эпоху трудно переоценить значимость, а соответственно, и стоимость цифровых ресурсов, требование выкупа под угрозой их повреждения либо уничтожения пока уголовно ненаказуемо, а предусмотренная уголовным законом ответственность за использование вредоносных программ по ст. 272 и 273 УК РФ не соответствует общественной опасности рассматриваемого деяния.

Сходным образом складывается ситуация с противоправными действиями, связанными с проведением DDoS-атак (сокращение от англ. Distributed Denial of Service — распределенная атака типа «отказ в обслуживании») [20], когда за прекращение блокирования доступа к информационной системе злоумышленники требуют передачу чужого имущества. В ходе такой атаки большое количество зараженных специальной вредоносной программой компьютеров пользователей, объединенных в одну бот-сеть, начинает генерировать паразитный сетевой трафик на целевой информационный ресурс, в результате чего атакуемая компьютерная система, будучи не в состоянии обработать аномально возросшее количество запросов, вынужденно прекращает обрабатывать запросы добропорядочных пользователей. Недостаточность эффективности противодействия такой угрозе за-

ключается также в том, что для осуществления DDoS-атаки могут быть использованы не зараженные вредоносной программой компьютеры пользователей, что позволило бы квалифицировать эти действия по ст. 272 и 273 УК РФ, а арендованные злоумышленниками у провайдеров хостинговых услуг вычислительные мощности, на которых они размещают соответствующее ПО. Сокрытие следов их деятельности обеспечивается применением специального способа в организации DDoS-атаки — через усиление и отражение (англ. Amplification/Reflection), позволяющего скрыть сетевые элементы злоумышленников. Механизм атаки заключается в том, что ПО, установленное на серверах злоумышленников, направляет запросы уязвимому стороннему серверу, при этом в запросах производится подмена исходного IP-адреса на адрес атакуемого ресурса. В результате сторонний сервер, отвечая на запросы, посылает на атакуемый ресурс пакеты, значительно большие по размеру, чем сами запросы, что и приводит к отказу в обслуживании. При этом действия злоумышленников остаются уголовно ненаказуемыми, так как несанкционированный доступ к компьютерной системе пользователя при таком способе совершения DDoS-атаки отсутствует.

Подводя итог краткому анализу развития, классификации и особенностей вредоносных программ, надо признать, что они соответствуют современному технологическому и функциональному уровню легального ПО. Прогнозируя его дальнейшее развитие в свете закономерностей продвижения компьютерных технологий и перемещения вычислительных и информационных ресурсов пользователей из локальных систем в облачные, можно ожидать разработку новых и адаптацию уже проверенных в преступной деятельности инструментов с целью осуществления атак на облачные вычислительные мощности крупных компаний [21]. Пока это кажется маловероятным в связи с тем уровнем защиты, который обеспечивается для безопасной обработки и хранения данных. Однако еще не так давно маловероятными казались неединичные успешные атаки на крупные хорошо защищенные компьютерные сети. Но на сегодняшний день целевые атаки на корпоративные сети с применением специально разработанного для этих целей вредоносного ПО стали едва ли не обыденностью в новостной ленте. Тем более важным представляется исследование подобной тематики с целью прогнозирования развития криминогенной ситуации в сфере компьютерной информации и своевременной разработки эффективных предупредительных мер противодействия такого вида преступности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Россинская Е.Р. Криминалистика : учебник / Е.Р. Россинская. — Москва : Норма — Инфра-М, 2016. — 464 с.

2. Россинская Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности / Е.Р. Россинская // Вестник Восточно-Сибирского института МВД России. — 2019. — № 2 (99). — С. 193–202.

3. Россинская Е.Р. Современные способы компьютерных преступлений и закономерности их реализации / Е.Р. Россинская, И.А. Рядовский // Lex Russica. — 2019. — № 3 (148). — С. 87–99.

4. Комментарий к Уголовному кодексу Российской Федерации. Особенная часть / под ред. Ю.И. Скуратова, В.М. Лебедева. — Москва : Норма — Инфра-М, 1996. — 592 с.

5. Lefferts R. Partnering with the AV Ecosystem to Protect our Windows 10 Customers // Microsoft. — 2017. — 20 June. — URL: https://www.microsoft.com/security/blog/2017/06/20/partnering-with-the-av-ecosystem-to-protect-our-windows-10-customers.

6. Нефёдова М. Mac перестали загружаться из-за обновления Google Chrome / М. Нефёдова // Xakep.ru. — URL: https://xakep.ru/2019/09/27/chrome-var-bug.

7. Русскевич Е.А. Понятие вредоносной компьютерной программы / Е.А. Русскевич // Актуальные проблемы российского права. — 2018. — № 11 (96). — С. 207–215.

8. Россинская Е.Р. К вопросу о частной криминалистической теории информационно-компьютерного обеспечения криминалистической деятельности / Е.Р. Россинская // Известия Тульского государственного университета. Экономические и юридические науки. — 2016. — № 3-2. — С. 109–117.

9. Computer Viruses and Other Malicious Software: A Threat to the Internet Economy / A. Plonk, A. Carblanc, M. van Eeten [et al.]. — Paris : OECD, 2009. — 244 p.

10. Rankin B. How Malware Works — Malicious Strategies and Tactics / B. Rankin // Lastline. — 2018. — 10 May. — URL: https://www.lastline.com/blog/how-malware-works-malicious-strategies-and-tactics.

11. Custers B. Banking Malware and the Laundering of its Profits / B. Custers, R. Pool, R. Cornelisse // European Journal of Criminology. — 2019. — № 16 (6). — P. 728–745.

12. Integrating Complex Event Processing and Machine Learning: An Intelligent Architecture for Detecting IoT Security Attacks / J. Roldan, J. Boubeta-Puig, J. Luis Martínez, G. Ortiz // Expert Systems with Applications. — 2020. — Vol. 149. — P. 113251.

13. Методические рекомендации по расследованию преступлений в сфере компьютерной информации : учеб. пособие / под ред. И.Г. Чекунова. — 2-е изд. — Москва : Изд-во Моск. ун-та МВД России им. В.Я. Кикотя, 2019. — 105 с.

14. Paul J.D. Review and Analysis of Ransomware Using Memory Forensics and Its Tools / J.D. Paul, J. Norman // Smart Intelligent Computing and Applications : Materials of Conference, Singapore, 27 Sept. 2019. — Singapore, 2019. — P. 505–514.

15. Smith B. The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack / B. Smith // Microsoft.com. — 2017. — 14 May. — URL: https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack.

16. Nashilov E. Троян RTM атакует российские организации / E. Nashilov // ThreatPost. — 2018. — 20 апр. — URL: https://threatpost.ru/rtm-banking-trojan-campaign-in-russia-december-2018/29602.

17. Zeltser L. The History of Fileless Malware — Looking Beyond the Buzzword / L. Zeltser // Zeltser.com. — URL: https://zeltser.com/fileless-malware-beyond-buzzword.

18. Левцов В. Анатомия таргетированной атаки / В. Левцов // Kaspersky.ru. — 2016. — 16 дек. — URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388.

19. Wyke J. The Current State of Ransomware / J. Wyke, A. Ajjan // Sophos.com. — 2015. — 22 Dec. — URL: https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-current-state-of-ransomware.pdf.

20. Spring T. ThreatList: Latest DDoS Trends by the Numbers / T. Spring // Threatpost. — 2019. — 7 Febr. — URL: https://threatpost.com/threatlist-latest-ddos-trends-by-the-numbers/141614.

21. Singh D.J. Detection of Malicious Software by Analyzing the Behavioral Artifacts Using Machine Learning Algorithms / D.J. Singh, J. Singh // Information and Software Technology. — 2020. — Vol. 121. — P. 106273.

REFERENCES

1. Rossinskaya E.R. *Kriminalistika* [Criminalistics]. Moscow, Norma Publ., Infra-M Publ., 2016. 464 p.

2. Rossinskaya E.R. Theory of Information and Computer Support of Criminalistic Activity: Concept, System, Basic Patterns. *Vestnik Vostochno-Sibirskogo instituta MVD Rossii = Vestnik of the Eastern Siberia Institute of the Ministry of the Interior of the Russian Federation*, 2019, no. 2 (99), pp. 193–202. (In Russian).

3. Rossinskaya E.R., Ryadovskiy I.A. Modern Means of Committing Computer Crimes and Patterns of their Execution. *Lex Russica*, 2019, no. 3 (148), pp. 87–99. (In Russian).

4. Skuratov Yu.I., Lebedev V.M. (eds.). *Kommentarii k Ugolovnomu kodeksu Rossiiskoi Federatsii. Osobennaya chast'* [Commentary on the Criminal Code of the Russian Federation. Special Part]. Moscow, Norma Publ., Infra-M Publ., 1996. 592 p.

5. Lefferts R. Partnering with the AV Ecosystem to Protect our Windows 10 Customers. *Microsoft*, 2017, June 20. Available at: https://www.microsoft.com/security/blog/2017/06/20/partnering-with-the-av-ecosystem-to-protect-our-windows-10-customers.

6. Nefedova M. Mas Stopped Loading due to Google Chrome Update. *Hacker.ru.* Available at: https://xakep.ru/2019/09/27/chrome-var-bug. (In Russian).

7. Russkevich E.A. Malicious Computer Program. *Aktual'nye problemy rossiiskogo prava = Topical Problems of Russian Law*, 2018, no. 11 (96), pp. 207–215. (In Russian).

8. Rossinskaya E.R. The Issue of Private Theory of Information and Computer Software Criminalistics Operations. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki = Izvestiya of the Tula State University. Economic and Legal Sciences,* 2016, no. 3-2, pp. 109–117. (In Russian).

9. Plonk A., Carblanc A., Eeten M. van [et al.]. *Computer Viruses and other Malicious Software: A Threat to the Internet Economy*. Paris, OECD Publ., 2009. 244 p.

10. Rankin B. How Malware Works — Malicious Strategies and Tactics. *Lastline*, 2018, May 10. Available at: https://www.lastline.com/blog/how-malware-works-malicious-strategies-and-tactics.

11. Custers B., Pool R., Cornelisse R. Banking Malware and the Laundering of its Profits. *European Journal of Criminology*, 2019, no. 16 (6), pp. 728–745.

12. Roldan J., Boubeta-Puig J., Luis Martínez J., Ortiz G. Integrating Complex Event Processing and Machine Learning: An Intelligent Architecture for Detecting IoT Security Attacks. *Expert Systems with Applications*, 2020, vol. 149, pp. 113251.

13. Chekunov I.G. (ed.). *Metodicheskie rekomendatsii po rassledovaniyu prestupleniy v sfere kompyuternoy informatsii* [Guidelines for the Investigation of Crimes in the Field of Computer Information]. 2nd ed. Moscow University of the Ministry of the Interior of Russia named after V.J. Kikot Publ., 2018. 105 p.

14. Paul J.D., Norman J. A Review and Analysis of Ransomware Using Memory Forensics and Its Tools. *Smart Intelligent Computing and Applications. Materials of Conference, Singapore, 2019, September 27*. Singapore, 2019, pp. 505–514.

15. Smith B. The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack. *Microsoft.com*, 2017, May 14. Available at: https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack.

16. Nashilov E. RTM Trojan Attacks Russian Organizations. *ThreatPost*, 2018, April 20. Available at: https://threatpost.ru/rtm-banking-trojan-campaign-in-russia-december-2018/29602.

17. Zeltser L. The History of Fileless Malware — Looking Beyond the Buzzword. *Zeltser.com.* Available at: https://zeltser.com/fileless-malware-beyond-buzzword.

18. Levtsov V. Anatomy of a Targeted Attack. *Kaspersky.ru*, 2016, December 16. Available at: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388. (In Russian).

19. Wyke J., Ajjan A. The Current State of Ransomware. *Sophos.com*, 2015, December 22. Available at: https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-current-state-of-ransomware.pdf.

20. Spring T. ThreatList: Latest DDoS Trends by the Numbers. *Threatpost*, 2019, February 7. Available at: https://threatpost.com/threatlist-latest-ddos-trends-by-the-numbers/141614.

21. Singh D.J., Singh J. Detection of Malicious Software by Analyzing the Behavioral Artifacts Using Machine Learning Algorithms. *Information and Software Technology*, 2020, vol. 121, pp. 106273.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Россинская Елена Рафаиловна — директор Института судебных экспертиз, заведующий кафедрой судебных экспертиз Московского государственного юридического университета им. О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, заслуженный деятель науки Российской Федерации, почетный работник высшего профессионального образования Российской Федерации, академик РАЕН, г. Москва, Российская Федерация; e-mail: elena.rossinskaya@gmail.com.

Рядовский Игорь Анатольевич — руководитель отдела расследования компьютерных инцидентов АО «Лаборатория Касперского», почетный работник прокуратуры Российской Федерации, г. Москва, Российская Федерация; e-mail: RyadIA@yandex.ru.

ДЛЯ ЦИТИРОВАНИЯ

Россинская Е.Р. Концепция вредоносных программ как способов совершения компьютерных преступлений: классификации и технологии противоправного использования / Е.Р. Россинская, И.А. Рядовский. — DOI: 10.17150/2500-4255.2020.14(5).699-709 // Всероссийский криминологический журнал. — 2020. — Т. 14, № 5. — С. 699–709.

INFORMATION ABOUT THE AUTHORS

Rossinskaya, Elena R. — Director, Forensic Expertise Institute, Head, Chair of Forensic Expertise, Kutafin Moscow State Law University (MSAL), Doctor of Law, Professor, Honored Researcher of the Russian Federation, Honored Worker of Higher Professional Education of the Russian Federation, Academician, Russian Academy of Natural Sciences, Moscow, the Russian Federation; e-mail: elena.rossinskaya@gmail.com.

Ryadovskiy, Igor A. — Head, Department of Investigating Computer Incidents, Kaspersky Lab Ltd., Honorary Worker of the Prosecutor's Office of the Russian Federation, Moscow, the Russian Federation; e-mail: RyadIA@yandex.ru.

FOR CITATION

Rossinskaya E.R., Ryadovskiy I.A. The concept of malware as a means of committing computer crimes: classification and methods of illegal use. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 5, pp. 699–709. DOI: 10.17150/2500-4255.2020.14(5).699-709. (In Russian).