СПОСОБЫ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Прусаков Д.А.
Email: Prusakov6117@scientifictext.ru

Прусаков Дмитрий Александрович – магистрант,
юридический факультет,
Рязанский государственный университет им. С.А. Есенина, г. Рязань

Аннотация: *развитие компьютерных технологий постоянно порождает развитие новых видов преступлений и способов их совершения и сокрытия.*
В связи с массовым распространением средств мобильной коммуникации возникли новые виды преступлений, такие как создание и распространение вредоносных программ для мобильных телефонов, использование мобильных средств связи для совершения мошенничеств, вымогательств, поджогов, взрывов, террористических актов и пр.
Ключевые слова: *информационно-компьютерное обеспечение, компьютерное преступление, механизм преступления, способ преступления, полноструктурный способ, неполноструктурный способ, вредоносная программа, несанкционированный доступ.*

METHODS OF COMPUTER CRIMES

Prusakov D.A.

Prusakov Dmitry Alexandrovich - Master's Student,
FACULTY OF LAW,
RYAZAN STATE UNIVERSITY S.A. YESENIN, RYAZAN

Abstract: *the development of computer technologies constantly gives rise to the development of new types of crimes and methods of their commission and concealment. In connection with the massive spread of mobile communications, new types of crimes have arisen, such as the creation and distribution of malicious programs for mobile phones, the use of mobile communications to commit fraud, extortion, arson, explosions, terrorist acts, etc.*
Keywords: *information and computer support, computer crime, crime mechanism, crime method, full-structured method, non-structured method, malicious program, unauthorized access.*

Описание способов совершения компьютерных преступлений начнем с действий по сокрытию преступниками своих данных при использовании интернета с целью предотвращения установления их личности.

Чтобы скрыть свой адрес, преступники используют различные анонимные компьютерные сети и специально созданные для этого сервисы.

Одним из таких способов является использование VPN-сервисов (англ. Virtual Private Network - виртуальная частная сеть)[1].

Технология VPN обеспечивает шифрование сетевого трафика между компьютером пользователя и VPN прокси-сервером, который является шлюзом в Интернет и, соответственно, скрывает реальный IP-адрес пользователя. Если требуется высокий уровень секретности, преступники арендуют вычислительные мощности у хостинг-провайдеров практически в любой точке мира, на которых они устанавливают свои собственные VPN-серверы или виртуальные машины, с которых, используя сторонние VPN-сервисы, они получают доступ в интернет.

Еще одним методом, позволяющим скрыть свой IP-адрес, является Onion Routing, TOR (второе поколение onion routing), технология и программное обеспечение для обмена данными с многослойным шифрованием с использованием системы прокси-серверов, обеспечивающих анонимное сетевое соединение[2].

Троянская программа, обладающая функциональными возможностями VPN-прокси-сервера, также позволяет преступникам создать бот-сеть из компьютеров, зараженных такой программой, и использовать ее для сокрытия своего IP-адреса.

Помимо упомянутых способов анонимизации своих действий в сети Интернет путем построения цепочки прокси-серверов, преступники для этих целей применяют и другие криминальные либо полукриминальные схемы, например через несанкционированное подключение к сторонним беспроводным точкам доступа (Wi-Fi-роутерам) или с помощью беспроводных модемов мобильной связи с сим-картами, оформленными на посторонних лиц.

Выбор безопасных способов оплаты услуг и вычислительных мощностей для преступной деятельности также является мерой корреляции преступной деятельности. Для этих целей широко используется так

[1] Куроуз Д., Росс К. Компьютерные сети: нисходящий подход. 6-е изд. М., 2016. С. 794 - 795.
[2] Ligh M., Adair S., Hartstein B., Richard M. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Indianapolis, 2010. Pp. 2 - 5.

называемая криптовалюта, например биткоин, правовой режим которой во многих странах мира, в том числе и в России, остается неопределенным.

Разработка планов преступной деятельности, координация действий на стадии подготовки к совершению преступления, координация совместных действий осуществляются сообщниками с использованием сетевых протоколов обмена сообщениями, обеспечивающих безопасность передачи данных.

Одной из наиболее востребованных реализаций коммуникации в криминальной среде является XMPP-протокол (extensible Messaging and Presence Protocol) обмена мгновенными сообщениями, известный еще как Jabber-протокол (буквально - болтовня), который предоставляет возможность настроить свой собственный Jabber-сервер, обеспечивающий шифрование канала[3].

Меры по сокрытию следов преступления могут также включать средства, с помощью которых преступники сопротивляются исследованию и изъятию компьютерной информации, содержащейся в их компьютерных средствах и системах криминалистического значения. Эти цели достигаются путем шифрования компьютерных данных с помощью специального программного обеспечения или путем быстрого уничтожения таких данных с помощью специальных программ или устройств.

Для сокрытия следов несанкционированного доступа и вредоносной активности на компьютере пользователя применяются различные меры технического характера, как прошедшие проверку временем технологии шифрования (криптования) и обфускации (obfuscate - делать неочевидным, запутанным), так и новые приемы и методы - "бестелесная" технология, технологии Bootkit, Rootkit и т.п.

Во время криптографии исполняемый код вредоносной программы шифруется, а во время обфускации он сводится к форме, затрудняющей анализ и понимание ее алгоритмов. Это затрудняет антивирусному программному обеспечению обнаружение таких программ, а специалистам по информационной безопасности-их расследование.

Вредоносное програмное обеспечение, которое функционирует только в оперативной памяти компьютера и не сохраняется на энергонезависимых запоминающих устройствах, называется "бестелесным". При выключении питания компьютера, например при перезапуске, программа стирается. Такие программы используются преступниками для сокрытия своей активности от антивирусных программ[4].

Технология Bootkit применяется для сокрытия вредоносного кода от антивирусного программного обеспечения и для получения максимальных привилегий в системе. Для реализации этого способа вредоносной программой модифицируется, например, главная загрузочная запись (англ. master boot record, MBR), которая считывается процессором еще до начала загрузки операционной системы, а вредоносный код в зашифрованном виде записывается в не используемую операционной системой область дискового пространства. При включении компьютера загрузчик еще до старта операционной системы расшифровывает и загружает в оперативную память вредоносный код[5].

Максимальные права пользователя позволяют применить набор программ Rootkit, которые скрывают вредоносную активность в системе: сетевые подключения, процессы, файлы и т.д.

Как видно из перечисленных мер, предпринимаемых преступниками с целью сокрытия следов несанкционированного доступа к компьютерным системам и информации пользователя, весьма значительное количество таких деяний совершается с помощью вредоносного программного обеспечения. Преступники используют вредоносные программы для значительного усиления своих возможностей, то есть в криминалистическом плане вредоносная программа является орудием совершения преступления[6].

В уголовно-правовом смысле определение вредоносного программного обеспечения определено в статье 273 УК РФ[7], согласно которой под вредоносным программным обеспечением понимается программа для ЭВМ или иная компьютерная информация, умышленно предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Такие программы должны включать в себя не только специально разработанное, но и модифицированное юридическое программное обеспечение, дополнительный функционал которого, вследствие модификации, придает ему признаки вредоносного ПО.

Отметим, что в качестве инструмента совершения преступления также может быть использована юридическая программа, функциональность которой предоставляет преступникам возможность достижения своих целей. Большинство легальных программ, используемых преступниками в незаконной деятельности, предназначены для удаленного несанкционированного доступа к компьютеру, управления системой и администрирования, например: RMS, Ammyy Admin, TeamViewer и LiteManager. Эти программы обладают

---

[3] Торичко Р.С., Клишина Н.Е. Некоторые вопросы совершенствования действующего законодательства, регламентирующего расследование киберпреступлений // Вестник экономической безопасности. 2018. N 3. С. 181.

[4] Zeltser L. The History of Fileless Malware - Looking Beyond the Buzzword. URL: https://zeltser.com/fileless-malware-beyond-buzzword (дата обращения: 05.01.2019).

[5] Matrosov A., Rodionov E., Bratus S. Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats. No Starch Press, 2015. P. 304.

[6] Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2017. N 1. С. 9 - 22.

[7] Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ (с изм. и доп.) // Собрание Законодательства Российской Федерации. 1996, №33(Часть I). Ст. 3431.

функциональными возможностями, достаточными для достижения преступных целей, и определяются антивирусным программным обеспечением с менее критичным именем как условно опасные, в связи с чем пользователи не видят в них особой угрозы. Кроме того, многие из этих программ являются доверенными программами пользователя, установлены с его ведома и не вызывают у него подозрений.

На этой основе способы компьютерных преступлений в зависимости от доступа к компьютерным средствам и системам можно подразделить:

- на способы, связанные с удаленным доступом к компьютерным средствам и системам посредством использования компьютерной коммуникационной сети (локальной или глобальной - Интернет);

- способы, связанные с непосредственным доступом к компьютерным средствам и системам.

В других случаях вовлечение потерпевшего в той или иной степени является необходимым условием для завершения преступных намерений. Непосредственная эксплуатация уязвимостей человеческого фактора предполагает непосредственное общение с жертвой с использованием навыков социальной инженерии, т. е. система психологических приемов и методов, склоняющих потерпевших к совершению определенных действий в интересах преступников, например, раскрыть уникальный код, отправленный в SMS-сообщении для авторизации на сетевом ресурсе, или самостоятельно загрузить программу удаленного администрирования на свой компьютер и предоставить данные доступа мошеннику.

Однако низкий уровень культуры информационной безопасности позволяет преступникам получать необходимую информацию для проведения атаки без непосредственного общения с жертвой. Использование ненадежных паролей, заводских настроек, программно-аппаратных конфигураций предоставляет широкий спектр возможностей для получения несанкционированного доступа к конфиденциальной информации. Таким образом, одним из широко известных и используемых способов получения несанкционированного доступа к компьютерной сети является проведение атаки с использованием различных способов блокирования портов узлов сети, т. е. виртуальные точки входа и выхода сетевого трафика, обслуживающие определенные локальные сервисы. После обнаружения открытого порта, который обычно используется одной из наиболее распространенных программ удаленного администрирования, преступники могут получить доступ к системе, выполнив поиск деталей доступа (пар логин и пароль).

Для доступа к корпоративным компьютерным системам преступники также могут воспользоваться уязвимостями в системах безопасности организации и регламентах предприятия, которые могут выражаться как в физическом проникновении за охраняемый периметр, так и в удаленном доступе с использованием протоколов и программного обеспечения, разрешенных в организации.

В связи с этим можно разграничить способы получения несанкционированного доступа к компьютерным системам и сетям по степени вовлеченности потерпевшего в этот процесс:

- эксплуатация уязвимостей аппаратного и программного обеспечения;

- использование недостатков организационного и технического характера корпоративных охранных систем;

- применение методов социальной инженерии.

Подводя итог, хотелось бы отметить, что в связи с продолжающимся бурным развитием информационно-коммуникационных технологий, в том числе криптографии, такая же динамика наблюдается и в развитии компьютерных преступлений, связанных с несанкционированным доступом преступников к компьютерным средствам и системам.

Мы полагаем, что анализ методов компьютерных преступлений, представленный в данной статье, наглядно показывает, что методы компьютерных преступлений полностью структурированы. Основной криминалистической закономерностью формирования и осуществления способа совершения преступления с использованием информационно-компьютерных технологий является то, что подготовка обычно предполагает действия по сокрытию, то есть сокрытию. при совершении компьютерных преступлений, связанных с несанкционированным доступом, для преступников характерно осуществление комплекса мер, предшествующих покушению на совершение преступления, которые также направлены на сокрытие его последствий.

Применительно к способам компьютерных преступлений можно обозначить следующие закономерности частной теории информационно-компьютерного обеспечения криминалистической деятельности:

- закономерности формирования и реализации способа преступления, совершаемого с использованием информационных компьютерных технологий (связь способа с личностью преступника, зависимость способа от конкретных обстоятельств совершения преступления и т.д.);

- закономерности отражения в компьютерных средствах и системах информации о связях действий и их результатов, повторяемости действий в похожих ситуациях, стереотипах действий субъектов при совершении преступлений;

- закономерности возникновения и развития обстоятельств, связанных с преступлением, сопряженным с использованием компьютерных средств и систем (как до, так и после его совершения), и значимых для расследования.

Список литературы / References

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (с изм. и доп.) // Собрание Законодательства Российской Федерации, 1996. № 33(Часть I). Ст. 3431.
2. *Куроуз Д., Росс К.* Компьютерные сети: нисходящий подход. 6-е изд. М., 2016. С. 794-795.
3. *Ligh M., Adair S., Hartstein B., Richard M.* Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Indianapolis, 2010. Pp. 2-5.
4. *Торичко Р.С., Клишина Н.Е.* Некоторые вопросы совершенствования действующего законодательства, регламентирующего расследование киберпреступлений // Вестник экономической безопасности, 2018. № 3. С. 181.
5. *Zeltser L.* The History of Fileless Malware - Looking Beyond the Buzzword. [Электронный ресурс]. Режим доступа: https://zeltser.com/fileless-malware-beyond-buzzword/ (дата обращения: 05.01.2019).
6. *Matrosov A., Rodionov E., Bratus S.* Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats. No Starch Press, 2015. P. 304.
7. *Чекунов И.Г.* Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность, 2017. № 1. С. 9-22.