Лебедева Анна Андреевна
канд. юрид. наук, доцент
ФГКОУ ВО «Московская академия
Следственного комитета Российской Федерации»
г. Москва

ПОРНО-ВЫМОГАТЕЛЬСТВО («SEXTORTION») – СПОСОБЫ СОВЕРШЕНИЯ

Аннотация*: в статье нашло анализируется способ совершения «порно-вымогательства» («sextortion») – базового элемента криминалистической характеристики, детальное рассмотрение которого необходимо для практики расследования рассматриваемой категории преступления.*

Ключевые слова*: вымогательство, криминалистическая характеристика, расследование, интернет рассылка, порно контент.*

Так называемое «Порно-вымогательство» по средствам электронных отправлений известно с 2018 года, однако и в 2021 действия злоумышленников стали изощрённее.

Рассматриваемый вид общественно опасного деяния получил распространение в зарубежных государствах и, охватывается англоязычным термином – «sextortion», который в буквальном смысле интерпретируется как, шантаж, связанный с разоблачениями из чьей-то личной половой жизни [7].

«Sextortion» – представляет собой алгоритм преступных действий по рассылке на электронную почту жертвы информационных писем, с целью принудительного изъятия имущества последней, под предлогом распространения позорящих сведений.

Чтобы обезопасить себя, преступники предлагают жертве суммы так называемого «выкупа» перечислить на криптокошелек, ранее преобразовав в финансовые цифровые активы.

В соответствии с национальным уголовным законодательством «Sextortion» квалифицируется в соответствии с нормами ст.ст. 163 УК РФ, 272 УК РФ, 138 УК РФ.

С учетом диспозиций статей 146 и 151 УПК РФ, положений Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации» №59-ФЗ, решение о возбуждении уголовного дела по соответствующим заявлениям правомочен принимать следователь СК России.

Верховный Суд Российской Федерации разъясняет, что угроза, которой сопровождается требование при вымогательстве, должна восприниматься потерпевшим как реальная, однако не приводит примеров, когда угроза может восприниматься таковой, и не указывает критерии реальности. В этой связи возможен отказ в возбуждении уголовного дела и непризнание судами «порно-вымогательств» преступлениями. Потерпевшие воспринимают «порно-вымогательство» в качестве реальной угрозы, тогда как сотрудники правоохранительных органов на практике соглашаются с этим только тогда, когда угроза подкрепляется фактическим компроматом, т.е. порно фото/видео.

Способ совершения: полноструктурный т. е. подразумевает действия по приготовлению, реализации преступного умысла, сокрытию преступления.

1. Подготовка к совершению рассматриваемого вида преступления предполагает наличие специальных компьютерных навыков, необходимых для получения *несанкционированного доступа* к почтовым аккаунтам предполагаемых потерпевших, путем незаконного приобретения, получения охраняемых законом персональных данных пользователей, в том числе паролей, логинов, почтовых серверов.

Так, согласно Приказа Минтруда России №348н «Об обработке персональных данных в Министерстве труда и социальной защиты Российской Федерации» адрес электронной почты отнесен к персональным данным.

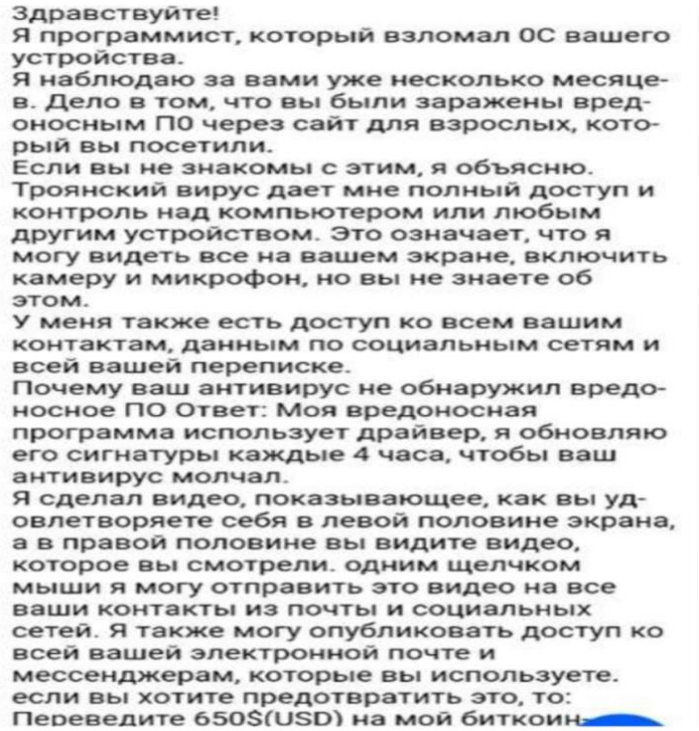
А Суды отказывают в удовлетворении ходатайств об истребовании логина и пароля электронного почтового ящика, обосновывая выводы наличием в переписке персональных данных как владельца почты, так и третьих лиц [3].

Если злоумышленник не знаком с потенциальной жертвой «порно- вымогательства», а умысел направлен на случайных пользователей почтовых сервисов, выбранных рандомно, то используются базы данных держателей почтовых ящиков, украденные и незаконным образом размещенные на информационных ресурсах в том числе и в «теневом» сегменте Сети Интернет.

Так одна из массовых «утечек» паролей почтовых серверов «yandex» (к аккаунту на Яндексе могут быть привязаны электронные кошельки) и «mail.ru» произошла в сентябре 2014 года, а в июле 2018 года поисковые системы предоставляли данные и пароли пользователей, хранящиеся в «Google Docs» [11].

Так, «О» в феврале 2015 года, имея умысел, направленный на неправомерный доступ к охраняемой законом компьютерной информации, используя находящуюся по адресу : <адрес> компьютерную технику – ПК с установленным жестким диском «Western Digital», серийный номер №, в ходе электронной переписки с помощью электронной компьютерной программы QIP, используя учетную запись в данной программе №, вступил в предварительный преступный сговор с неустановленным следствием лицом, находящимся в неустановленном следствием месте, осуществляющим электронную переписку с помощью электронной компьютерной программы QIP с учетной записью №, на совершение неправомерного доступа к охраняемой законом компьютерной информации – а именно, информации о пароле <данные изъяты>, соответствующему электронному почтовому ящику <данные изъяты>.ru, принадлежащему законному владельцу, хранящейся на компьютерах пользователей <данные изъяты>.ru, преследуя цель дальнейшего использования логинов и паролей к электронным почтовым ящикам <данные изъяты>ru, <данные изъяты>.ru [5].

2. Реализация преступного умысла. Направление непосредственно электронного сообщения, в тексте которого содержатся сведения об осведомленности злоумышленника о «позорящих» потенциального потерпевшего действиях, событиях, а также форме и размере имущества, способе его передаче, для целей не придания гласности компрометирующей информации.


Здравствуйте!
Я программист, который взломал ОС вашего устройства.
Я наблюдаю за вами уже несколько месяцев. Дело в том, что вы были заражены вредоносным ПО через сайт для взрослых, который вы посетили.
Если вы не знакомы с этим, я объясню.
Троянский вирус дает мне полный доступ и контроль над компьютером или любым другим устройством. Это означает, что я могу видеть все на вашем экране, включить камеру и микрофон, но вы не знаете об этом.
У меня также есть доступ ко всем вашим контактам, данным по социальным сетям и всей вашей переписке.
Почему ваш антивирус не обнаружил вредоносное ПО Ответ: Моя вредоносная программа использует драйвер, я обновляю его сигнатуры каждые 4 часа, чтобы ваш антивирус молчал.
Я сделал видео, показывающее, как вы удовлетворяете себя в левой половине экрана, а в правой половине вы видите видео, которое вы смотрели. одним щелчком мыши я могу отправить это видео на все ваши контакты из почты и социальных сетей. Я также могу опубликовать доступ ко всей вашей электронной почте и мессенджерам, которые вы используете.
если вы хотите предотвратить это, то:
Переведите 650$(USD) на мой биткоин

В соответствии с Постановлением Пленума Верховного Суда РФ от 17.12.2015 №56, касающемся судебной практики по делам о вымогательстве [6], под позорящими данными следует понимать сведения, порочащие честь, достоинство или подрывающие репутацию лица или его близких (фото/видео изображения аморального поступка, в том числе информации о приватном посещении «порно контента»). При этом значения не имеет, соответствуют ли действительности сведения, под угрозой распространения которых совершается вымогательство.

Для придания реальности содержавшейся в электронном сообщении информации, с целью формирования у жертвы «порно-вымогательства» подлинного представления о возможности распространения компрометирующей ее информации о пользовании «порно контентом», злоумышленник детально расписывает где, как и каким образом получил так называемый «компромат», путь его возможного распространения, а также способ передачи имущества жертвы в обмен на «сохранения личной тайны».

Так, злоумышленник, вводя в заблуждение, сообщает, что незаконным образом получил доступ и удаленным способом активировал Web-камеру персонального компьютера, создал видеофайл, содержащий смонтированные кадры

порнографического видео, а также видео действий самого скомпрометированного лица, в момент пребывания на порно-ресурсе.

В ряде случаях вымогатели предлагают жертвам самостоятельно убедиться в реальности угрозы распространения порочащих фото/видео файлов, указывая электронный адрес ссылки на архив ZIP, в котором якобы содержатся компрометирующее пользователя видеоматериалы.

Однако в международной судебной практике имеются случаи привлечения к уголовной ответственности и за реальную «слежку с помощью Web-камеры ПК» и последующее «порно-вымогательство» по средствам электронной почты.

Так, Гражданин Кипра осужден на 4 года лишения свободы за незаконный доступ к Web -камере с целью скрытого наблюдения за жизнью несовершеннолетней девушки.

47-летний компьютерщик незаконно создал и применил вредоносную компьютерную программу для получения удаленного контроля над Web-камерой жертвы. Персональный компьютер потерпевшей был «инфицирован» после того, как девушка открыла вложение из незнакомого письма, пришедшего на ее электронную почту.

Преступник, угрожая отправить незаконным образом, тайно сделанные приватные снимки друзьям жертвы, принуждал последнюю позировать обнаженной перед веб-камерой [8].

Однако, в большинстве случаев, у «порно-вымогателя» нет доступа к Web-камере персонального компьютера адресата.

Для введения в заблуждения, создания ложного представления о реальности угроз, злоумышленник используют адрес электронной почты жертвы в качестве адреса отправителя письма. Т.е. фактически жертва направила письмо с угрозами «сама себе».

С целью придания угрозе огласки большей убедительности злоумышленники, в ряде случаев, приводят в тексте сообщений пароли почтовых ящиков жертв, полученные по средствам различных утечек данных.

Следует отметить, что электронное письмо по протоколу SMTP (Simple Mail Transfer Protocol – простой протокол передачи почты) – общедоступный сетевой протокол, предназначенный для отправления электронной почты в сетях TCP/IP.) состоит из так называемого «конверта», «заголовков» и «содержания» письма. Информация о получателе (MAIL FROM) и отправителе (RCPT TO) размещена в «конверте», а также показывается в заголовках.

При помощи ввода стандартных команд протокола вымогатель имеет возможность внести изменения в адрес отправителя письма (RCPT TO) в заголовке и даже поменять обратный адрес. В этом случае в качестве обратного адреса письма будет транслироваться почта получателя, у которого, в свою очередь формируется ложное понимание реальности угрозы злоумышленника о возможности распространения, компрометирующих его информации и медиа файлов.

3. Сокрытие. Чтобы обезопасить себя, преступники предлагают жертве суммы так называемого «выкупа» перечислить на криптокошелек, ранее преобразовав в финансовые цифровые активы.

Ранее, до 2017 года вымогательство в криптовалюте по национальному законодательству не квалифицировалось в соответствии с нормами уголовного закона.

Однако судебная практика пошла по пути так называемой «легализации» цифровых финансовых активов- приравнивая их к категории иного имущества, ссылаясь на нормы Гражданского Кодекса РФ.

Так, в Определении Верховного суда Республики Башкортостан от 20.02.2017 г. №33–3487/2017 суд указал, что «виртуальная валюта», ... является не средством платежа за товар, а непосредственно товаром.

В Постановлении 9 Арбитражного Апелляционного суда от 15.05.2018г. №09АП-16416/2018 по делу №А40–124668/2017, по мнению суда, криптовалюта не может быть расценена применительно к ст. 128 ГК РФ иначе как иное имущество.

По мнению Председателя Следственного комитета Российской Федерации – «…признание финансовых цифровых активов (криптовалюты) в качестве

имущества для целей уголовного и уголовно-процессуального законодательства является необходимым условием расследования уголовных дел, по которым цифровая валюта выступает, например, предметом взятки или хищения» [10].

Таким образом в статье нашло отражение способа совершения «порно-вымогательства» («sextortion») – базового элемента криминалистической характеристики, детальный анализ которого необходим для практики расследования рассматриваемой категории преступления.

Список литературы

1. Федеральный закон от 02.05.2006 №59-ФЗ (ред. от 27.12.2018) «О порядке рассмотрения обращений граждан Российской Федерации»// Парламентская газета, №70–71, 11.05.2006

2. Приказ Минтруда России от 29.05.2014 №348н (ред. от 20.10.2020) «Об обработке персональных данных в Министерстве труда и социальной защиты Российской Федерации» (вместе с «Правилами обработки персональных данных в Министерстве труда и социальной защиты Российской Федерации») (Зарегистрировано в Минюсте России 01.09.2014 №33914) // первоначальный текст документа опубликован в издании «Российская газета», №296, 26.12.2014.

3. Постановления арбитражного суда Северо-Кавказского округа по делам об обжаловании определений об отказе в истребовании доказательств в виде данных логина и пароля почтовых ящиков должника по делу о банкротстве (от 16 августа 2019 г. по делу № А53–23516/2017, от 15 июля 2019 г. по делу № А53–23514/2017

4. Определение Верховного суда Республики Башкортостан от 20.02.2017 г. №33–3487/2017 [Электронный ресурс]. – Режим досупа: http://vs.bkr.sudrf.ru/ (обращения 16.01.21)

5. Приговор Центрального районного суда г. Челябинска по делу №1–141/2017 (ч. 3 ст. 272 УК РФ).

6. Постановление Пленума Верховного Суда РФ от 17.12.2015 №56 «О судебной практике по делам о вымогательстве (статья 163 Уголовного кодекса Российской Федерации)»// Источник публикации Российская газета, №294, 28.12.2015,

7. Cambridge English Pronouncing Dictionary, Cambridge University Press, 2011 – 580 page.

8. Хакер получил 4 года тюрьмы за взлом веб-камеры [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/news/356788.php (дата обращения: 02.02.2020).

9. Постановление 9 Арбитражного Апеляционного суда от 15.05.2018 г №09АП-16416/2018 [Электронный ресурс]. – Режим доступа: https://9aas.arbitr.ru/ (дата обращения: 16.01.21).

10. Интервью А.И. Бастрыкина от.08.12.20 [Электронный ресурс]. – Режим доступа: https://ria.ru/20201208/kriptovalyuta-1588242025.html (дата обращения: 16.01.21).

11. Благовещенский А. Данные пользователей Google попали в открытый доступ, статья от 05.07.2018 [Электронный ресурс]. – Режим доступа: https://rg.ru/2018/07/05/iandeks-sluchajno-vylozhil-v-otkrytyj-dostup-dannye-polzovatelej-google.html (дата обращения: 02.02.2021).

12. Интервью эксперта Лаборатории Касперского от 07.09.2014 [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/utekli-paroli-k-pochte-na-yandekse-i-mail-ru-pobochnyj-ushherb-bolshe-pryamogo (дата обращения 02.02.2021).