УДК 343.13
ББК 67.410.212

О некоторых проблемах предварительного расследования хищений денежных средств граждан с использованием вредоносных компьютерных программ

Д.В. Ким, Г.Е. Брызгалов

Барнаульский юридический институт МВД России (Барнаул, Россия)

Some Issues of the Preliminary Investigation of the Embezzlement of Citizens' Money Using Scumware

D.V. Kim, G.E. Bryzgalov

Barnaul Law Institute of the Ministry of Internal Affairs of Russia (Barnaul, Russia)

Статья посвящена актуальной на сегодняшний день проблеме осуществления предварительного расследования хищений денежных средств граждан с использованием вредоносных компьютерных программ. Целью работы является изучение вопросов, возникающих у сотрудников органов внутренних дел по уголовным делам данной категории. Авторами предпринимается попытка проанализировать основные проблемы, влияющие на результативность предварительного расследования.

Анализ судебно-следственной практики показывает, что предварительное расследование по указанной категории уголовных дел представляет особую сложность, заключающуюся в многоэпизодности преступной деятельности, длительном периоде совершения преступлений, отказе от сотрудничества со следствием задержанных лиц и свидетелей, в результате чего участники устанавливаются проведением большого объема следственных и иных процессуальных действий, а также оперативно-разыскных мероприятий.

В то же время успешному расследованию указанной категории дел способствует эффективное проведение оперативно-разыскных мероприятий и четко налаженное взаимодействие между следственными подразделениями, подразделениями органа дознания с оперативными и экспертно-криминалистическими подразделениями. Такое взаимодействие позволяет раскрыть преступную схему совершения преступлений в полном объеме, закрепить следы преступления и изобличить виновных лиц.

Ключевые слова: вредоносная компьютерная программа, мобильное устройство, предварительное расследование, первоначальный этап расследования, операционная система Android.

The article is devoted to the actual problem of the preliminary investigation of embezzlement of citizens' money using scumware. The purpose of the article is to investigate the issues arising for law enforcement agencies in criminal cases of this category. The authors attempt to analyze the main problems influencing the effectiveness of the preliminary investigation.

The analysis of the forensic investigation shows that the preliminary investigation in this category of criminal cases is particularly difficult. The complexity lies in multi-episodicity of criminal activity, the long period of commission of crimes, refusal to cooperate with the investigation of detainees and witnesses. As a result the participants in the crime are established by carrying out a large volume of investigative and other procedural actions as well as operational-search activities.

At the same time a successful investigation of this category of cases is facilitated by the effective conduct of operational and search activities and well-established interaction between investigative units, units of the body of inquiry with operational and expert-criminalistic units. Such interaction allows solving the criminal scheme of committing crimes in all parts, fixing the traces of the crime and exposing the guilty persons.

Key words: scumware, mobile device, preliminary investigation, initial stage of investigation, operating system "Android".

DOI 10.14258/izvasu(2018)3-32

Стремительные темпы развития современных информационных и финансовых технологий позволяют преступникам использовать новые платежные механизмы для получения доходов при минимальных затратах и рисках быть привлеченными к уголовной ответственности.

Так, по данным Банка России, об операциях, совершенных на территории Российской Федерации и за ее пределами с использованием платежных карт, эмитированных на территории Российской Федерации, количество и объем соответствующих операций неизменно увеличиваются. Рост показателей за 2017 г. составил около 25% относительно аналогичных значений за 2016 г. [1].

Согласно обзору, подготовленному специалистами «Лаборатории Касперского», по результатам 2017 г. банковское вредоносное программное обеспечение также расширило свой функционал, и в 2017 г. выявлено несколько новых методов, используемых для кражи денег. Одна из модификаций вредоносной компьютерной программы FakeToken атаковала более 2000 финансовых приложений. Эта вредоносная компьютерная программа перекрывает приложения фишинговыми окнами, предназначенными для кражи данных банковской карты пользователя. Обнаружены модификации FakeToken, атакующие приложения для вызова такси, заказа билетов, бронирования гостиниц и даже для оплаты штрафов за нарушение ПДД [2].

Указанное свидетельствует о том, что с увеличением количества мобильных устройств, расширением области их применения, ростом использования платежных карт и числа мобильных пользователей повышается вероятность активного развития вредоносных компьютерных программ.

Федеральным законом от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» УК РФ был дополнен статьей 159.6 [3]. В соответствии с новой нормой за хищение чужого имущества или приобретение права на чужое имущество посредством ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей предусмотрена уголовная ответственность, которая призвана защитить отношения собственности, имущественные интересы, отношения, обеспечивающие охрану компьютерной информации и безопасность информационно-телекоммуникационных сетей.

Данные официальной статистики свидетельствуют о том, что, несмотря на появление в УК РФ статьи 159.6, она практически не применяется правоохранительными органами, противоправные действия зачастую квалифицируются по ст. 158, 159 УК РФ [4]. При выявлении и расследовании преступлений данной категории наблюдаются ошибки и недочеты, в результате чего многие уголовные дела не доходят до судебного разбирательства.

Деятельность правоохранительных органов по указанным делам часто не результативна из-за отсутствия достаточного количества знаний у следователей, оперативных работников по расследованию уголовных дел о хищениях денежных средств, совершаемых с использованием вредоносных компьютерных программ и имеющихся научно-технических достижений в этой области. Так, Е.С. Шевченко в своем исследовании проводит опрос среди следователей (респондентами стали 170 следователей и 20 дознавателей), по результатам которого обнаруживается следующее: 95% респондентов имеют только юридическое образование, лишь 5% из числа опрошенных получили дополнительную подготовку, например образование по специальности «Информатика и вычислительная техника». 63% опрошенных оценивают уровень владения персональным компьютером как уровень «среднестатистического пользователя», 37% — «продвинутого пользователя». Источником получения знаний в области компьютерных технологий 79% опрошенных следователей назвали самообразование, 21% — курсы повышения квалификации сотрудников правоохранительных органов, 5% — коммерческие курсы или специальное образование [5, с. 29].

В предварительном расследованим по уголовным делам о хищениях денежных средств, совершаемых с использованием вредоносных компьютерных программ, главной целью для следователя является установление всех обстоятельств совершения преступления и сбор необходимых доказательств вины конкретных лиц.

При анализе стадии возбуждения уголовного дела о хищениях денежных средств с использованием вредоносных компьютерных программ у следователей часто возникают вопросы по установлению места совершения преступления, так как преступники пользуются мобильными устройствами с сим-картами, абонентские номера которых зарегистрированы на несуществующих индивидуальных предпринимателей, либо анкетные данные вымышлены полностью, что позволяет им длительное время находиться вне поля зрения правоохранительных органов.

Следователи в ходе предварительного расследования сталкиваются с проблемой установления всех эпизодов преступной деятельности виновного лица. Это обусловлено тем, что вредоносные компьютерные программы часто меняются, когда становятся неэффективными и уже не приносят стабильного дохода. Кроме того, в момент совершения преступления фигуранты активно передвигаются по территории Российской Федерации и стран СНГ,

осуществляя свою преступную деятельность на съемных квартирах. В целях конспирации банковские счета платежных карт и абонентские номера, к которым «привязаны» «Киви-кошельки» (через которые выводятся похищенные денежные средства, добытые преступным путем), регистрируются на подставных лиц. Преступники зачастую снимают похищенные денежные средства в других регионах Российской Федерации, постоянно меняют средства связи и пользуются программами, имеющими защиту в виде шифрования, что значительно затрудняет проведение оперативно-разыскных мероприятий, направленных на установление личности преступников и изобличение всех участников преступной группы.

Предварительное расследование по указанной категории уголовных дел представляет особую сложность, заключающуюся в многоэпизодности межрегиональной преступной деятельности, длительном периоде совершения преступлений, отказе от сотрудничества со следствием задержанных лиц в целях изобличения всех участников преступной группы, в результате чего участники устанавливаются проведением большого объема следственных и иных процессуальных действий, а также оперативно-разыскных мероприятий как на территории места дислокации органа предварительного следствия, так и за ее пределами. Кроме того, предварительное расследование затруднено длительностью (не менее месяца) предоставления информации от операторов сотовой связи, а также из банковских учреждений, находящихся в других субъектах Российской Федерации. При этом ответы на запросы приходят с большим объемом информации, которую необходимо проанализировать, что, в свою очередь, занимает много времени [6].

Одним из способов хищений денежных средств, совершаемых с использованием вредоносных компьютерных программ, является распространение указанных программ через интернет-магазины, такие как Google Play Store [7]. В ходе осуществления следственных и процессуальных действий, а также оперативно-разыскных мероприятий, направленных на установление лиц, осуществивших хищения денежных средств с использованием вредоносных компьютерных программ, не представляется возможности установить местонахождение компьютера, с которого осуществляется направление команд, так как компьютеру присваивается каждый раз динамический IP-адрес, который согласно ответам на запросы у провайдеров находится не на территории Российской Федерации.

Обозначенные выше проблемы в совокупности приводят к неполноте проведенного расследования и нарушению разумного срока досудебного производства, приостановлению предварительного следствия на основании п. 1 ч. 1 ст. 208 УПК РФ.

Зачастую расследование хищений денежных средств, совершаемых с использованием вредоносных компьютерных программ, производится несвоевременно. Одним из аспектов несвоевременности проведения необходимых следственных и иных процессуальных действий является отсутствие в уголовном деле плана расследования, согласованного с руководителями заинтересованных служб, либо наличие формально составленного плана, в результате чего не обеспечивается полнота проведения предварительного расследования [8].

Что касается взаимодействия следователя с органом дознания, то в данном аспекте также имеются недостатки, выражающиеся в том, что поручения следователей о проведении оперативно-разыскных мероприятий выполняются несвоевременно, а в случае выполнения зачастую имеются факты составления формальных справок об отсутствии значимой для следствия информации [9].

Особенность раскрытия указанных преступлений, а также установление дополнительных фигурантов организованной преступной группы происходит не в рамках сбора материала предварительной проверки, а в рамках производства предварительного следствия при проведении такого следственного действия, как осмотр изъятой компьютерной техники и цифровых носителей с участием эксперта [10].

Успешному раскрытию указанной категории преступлений, а также расследованию уголовных дел, сбору достаточного количества доказательств способствует эффективное проведение оперативно-разыскных мероприятий и четко налаженное взаимодействие между следственными подразделениями, подразделениями органа дознания с оперативными и экспертно-криминалистическими подразделениями на первоначальном этапе расследования. Это, в свою очередь, позволяет раскрыть преступную схему совершения преступлений в полном объеме, закрепить следы преступления и изобличить виновных лиц в совершении преступлений.

Библиографический список

1. Обзор несанкционированных переводов денежных средств за 2017 год // Банк России [Электронный ресурс]. — URL: https://www.cbr.ru/StaticHtml /File/14435/survey_transfers_17.pdf.

2. Эмм Д., Унучек Р.С. Kaspersky Security Bulletin: Обзор 2017. Развитие угроз [Электронный ресурс]. — URL: https://d2538mqrb7brka.cloudfront.net/wp-content/uploads/sites/58/2018/03/09043350/KSB_Review-of-2017 _final_RU.pdf.

3. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации : Федеральный закон от 29.11.2012 № 207-ФЗ [Электронный ресурс]. — URL: http://www.pravo.gov.ru.

4. Состояние преступности в России за январь-декабрь 2017 года, подготовленное ФКУ «ГИАЦ» МВД России [Электронный ресурс]. — URL: https://xn--b1aew.xn--p1ai/reports/item/12167987.

5. Шевченко Е.С. Актуальные проблемы расследования киберпреступлений // Эксперт-криминалист. — 2015. — № 3.

6. Уголовное дело № 1-18/2017 // Архив Октябрьского районного суда г. Барнаула.

7. Унучек Р.С. Мобильная вирусология 2017 [Электронный ресурс]. — URL: https://securelist.ru/mobile-malware-review-2017/88857/#comment-213356.

8. Уголовное дело № 360383 // Архив отдела по расследованию преступлений, совершенных на территории, обслуживаемой отделом полиции по Железнодорожному району СУ УМВД России по г. Барнаулу. — 2015.

9. Уголовное дело № 360282 // Архив отдела по расследованию преступлений, совершенных на территории, обслуживаемой отделом полиции по Железнодорожному району СУ УМВД России по г. Барнаулу. — 2015.

10. Гусев Д.В. Информационное письмо ЭКЦ МВД России «Особенности исследования информации в мобильных устройствах (ОС Android) по преступлениям в сфере дистанционного банковского обслуживания» // Архив контрольно-методического отдела ГСУ ГУ МВД России по Алтайскому краю. — 2016.