Аврамова Юлия Игоревна
Эксперт отдела компьютерных экспертиз,
ЭКЦ УМВД России по Мурманской области,
E-mail: obaiashka87@rambler.ru

Avramova Yuliya Igorevna
Expert of computer forensics Forensic Center
Ministry of Internal Affairs of Russia,
Murmansk region

ПРОИЗВОДСТВО ЭКСПЕРТИЗ И ИССЛЕДОВАНИЙ В ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКОМ ЦЕНТРЕ УМВД РОССИИ ПО МУРМАНСКОЙ ОБЛАСТИ ПО УГОЛОВНЫМ ДЕЛАМ, СВЯЗАННЫМ С ХИЩЕНИЕМ ДЕНЕЖНЫХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО БАНКИНГА

PERFORMANCE OF EXPERT EXAMINATIONS AND RESEARCHES IN THE FORENSIC CENTER OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA MURMANSK REGION ON CRIMINAL CASES RELATED TO EMBEZZLEMENT WITH THE USE OF MOBILE BANKING

Аннотация: В статье описывается общий ход исследования мобильных устройств по уголовным делам, связанным с хищением денежных средств с использованием мобильного банкинга. Сотрудникам ЭКЦ МВД России предлагается участвовать в формировании базы статистических данных посредством внесения в нее сведений по результатам производимых экспертиз и исследований. База позволит сократить сроки расследования уголовных дел, систематизировать работу экспертов.

Annotation: The article provides the general development of the mobile devices research in criminal cases related to embezzlement of funds using Mobile Banking. Employees of the Forensic Science Center MIA of Russia are provided to be engaged in the formation of a statistical database with data entry based on the results of ongoing examinations, studies that shorten time for the investigation, and systematize the work of experts.

Ключевые слова: мобильное устройство; физический образ; статический анализ; декомпиляция; источник управления; источник заражения; динамический анализ.

Keywords: mobile device; physical image; static analysis; decompilation; source of management; computer infection source , dynamic analysis.

В последние десятилетия информационные технологии активно входят в нашу жизнь, практически у каждого человека имеется универсальное устройство, вычислительная мощность которого превышает возможности компьютеров. К сожалению, уровень технической грамотности большинства населения остается достаточно низким, чем и пользуются злоумышленники.

В последние годы широкое распространение получили электронные банковские услуги, а некоторые банки полностью отказались от офисов (например, «Тинькофф») и предоставляют услуги дистанционно посредством программного обеспечения для смартфонов. Одной из популярных технологий является мобильный банкинг. С его помощью можно управлять своими счетами и картами, открывать и закрывать срочные вклады, настраивать регулярные платежи и СМС-оповещения, обменивать валюту и многое другое.

Несмотря на попытки банков повысить уровень безопасности предоставляемых услуг, сохраняется возможность перевода денежных средств между счетами и картами с использованием стандартной функции мобильных устройств (телефонов, планшетов) – отправки СМС-сообщений. В отличие от банковского программного обеспечения, уровень безопасности подобных операций довольно низкий. Существует два основных способа скомпрометировать управление банковским счетом на мобильном устройстве: использование социальной инженерии и «заражение» мобильного устройства специальным программным обеспечением.

С 2015 года по настоящее время в Мурманской области выявлено более 1 000 случаев мошенничества, связанных с хищением денежных средств через мобильный банк, предоставляемый ПАО «Сбербанк». В ЭКЦ УМВД России по Мурманской области было назначено более 700 экспертиз и исследований мобильных устройств.

При обращении граждан с жалобами на кражу денежных средств с их банковских счетов после проведения проверки возбуждаются уголовные дела по ч. 1 ст. 158 УК РФ. Затем лицом, проводящим проверку, изымается мобильный телефон потерпевшего и выносится постановление о назначении компьютерной экспертизы.

Исследование мобильных устройств проводится в соответствии с типовой методикой исследования информации в мобильных телефонах ЭКЦ МВД России 2013 года [1] в следующем порядке:

1. Получение доступа к области данных мобильного устройства, снятие физического дампа. Идеальный вариант – снятие физического образа.

2. Работа с физическим образом [2]:

а) восстановление удаленной информации;

б) поиск файлов, в т.ч. «*.apk», которые являются исполняемыми для операционной системы Android в системных или пользовательских областях памяти мобильного телефона, детектируемыми антивирусными программами (например, файл «Авито Фото.apk»).

3. Классификация выявленных файлов с помощью антивирусного программного обеспечения: «Kaspersky», «ESET-NOD32» или «Dr.Web», соотнесения с базами, актуальными на момент сканирования.

4. Статический анализ выявленных файлов (анализ программного обеспечения, производимый без реального выполнения исследуемых программ), в ходе которого проводится исследование файлов, в т.ч. извлечение данных из файлов «*.apk», декомпиляция представленного

программного обеспечения (трансляция исполняемого модуля в эквивалентный исходный код на языке программирования).

В процессе изучения данных, полученных после декомпиляции, эксперт устанавливает, на выполнение каких действий имеет разрешение исследуемое программное обеспечение, анализирует адреса ресурсов сети, с которыми оно взаимодействует в ходе работы, определяет источник «заражения» (каким образом вредоносное программное обеспечение попало на устройство, рис. 1).

```
HttpClient httpclient = new DefaultHttpClient();
HttpPost httppost = new HttpPost("http://" + new DbSet(Settings.context).getServer() + "/controller.php");
httppost.setEntity(new UrlEncodedFormEntity(nameValuePairs, "UTF8"));
```

```
public static String SERVER = "ghydiom14.com";
public static String USSD_NOTIFY = "ussd.notify";
public static String USSD_ON = "android.intent.action.ussd.on";
public static String VERSION = "Bot.v.4.2";
```

Рис. 1. Фрагменты кода с настройками (файл «classes.dex»)

5. Динамический анализ исследуемых файлов (анализ программного обеспечения в процессе запуска в реальной или виртуальной среде), в ходе которого проводится исследование на «заражаемой» «вирусом» тестовой операционной системе с установленным эмулятором Android.

В результате динамического анализа файла «*.apk» можно получить хеш-сумму файла (алгоритм SHA-256 предпочтительнее), установить, на выполнение каких действий имеет разрешение исследуемое программное обеспечение, и определить (выявить) IP-адреса, к которым обращается исследуемое программное обеспечение, например 162.222.213.25.

Практика производства экспертиз и исследований показывает, что «заражение» мобильного устройства, как правило, происходит следующими способами:

– при переходе по ссылкам, полученным в сообщениях, информация фиксируется в файле «<data>:\data\com.android.providers.telephony\databases\mmssms.db»;

– при поиске и установке на мобильное устройство программного обеспечения (приложений) не из «Play market» или «App Store», а из сторонних источников информация о загрузках может сохраняться в истории браузера, при этом фиксируются данные об источнике, имени самого файла и времени загрузки.

После «заражения» в ходе установки программного обеспечения на мобильном устройстве создается копия файла «*.apk» в разделе «DATA \ APP». Каталог «DATA» предназначен для хранения служебных данных. При этом в зависимости от функциональных возможностей мобильного устройства в указанном каталоге могут храниться:

– файлы баз данных со сведениями о перехваченных СМС;

– файлы, содержащие информацию о настройках программного обеспечения, в том числе имя сервера, логин, пароль, временные метки, указание номеров, с которых идет перехват СМС.

Таким образом, экспертами в ходе производства экспертиз и исследований о файлах, детектируемых (определяемых) программами-антивирусами как вредоносное программное обеспечение, собираются и анализируются следующие сведения:

– имя (например, «Авито Фото.apk»);

– на выполнение каких действий у него имеется разрешение (например, изменение СМС и ММС, отправка СМС-сообщений и др.);

– хеш-сумма (контрольная сумма), посчитанная по алгоритму SHA-256 (например, 10dcc538a97bd11526f5547147e68b50c5c172705aee726 fc9eaa9617cfe5fdf);

– источник «заражения» – номер телефона, с которого получена ссылка на файл (например, +456099248527), и/или интернет-ресурс (например, http://av1t.biz/v2);

– источник управления – сетевой адрес ресурса (сервера управления), с которым взаимодействует исследуемое программное обеспечение (например, IP-адрес 95.183.9.94 или доменное имя http://runopl.com).

Накопленные в ЭКЦ УМВД России по Мурманской области статистические данные показывают, что существует возможность объединения уголовных дел и материалов проверки в следующих случаях:

– общий источник «заражения»;

– общий источник, с которым взаимодействовало исследуемое программное обеспечение;

– совпадение контрольных сумм выявленных файлов.

В целях объединения уголовных дел и материалов проверки о фактах мошенничества, связанных с хищением денежных средств посредством мобильного банкинга с использованием СМС-сообщений, сотрудники ЭКЦ и органов дознания УМВД России по Мурманской области совместно участвуют в формировании общей базы статистических данных путем внесения в нее сведений, полученных в ходе расследования уголовных дел и по результатам проводимых экспертиз и исследований.

Предположительно, ведение этой базы позволит сократить сроки расследования уголовных дел, связанных с хищением денежных средств с использованием мобильного банкинга, систематизировать работу экспертов (уменьшить количество назначаемых экспертиз и исследований), улучшить взаимодействие между подразделениями, участвующими в расследовании указанных уголовных дел.

Список литературы

1. Типовая методика исследования информации, содержащейся в мобильных телефонах / О.В. Тушканова, В.М. Щербак, С.Н. Синицын, С.В. Ермолов. – М.: ЭКЦ МВД России, 2013.

2. Специальные знания, используемые при исследовании компьютерной информации: Учебное пособие / Ю.М. Баркалов. – ВИ МВД России, 2017.

3. Исследование памяти мобильных устройств с помощью специализированного комплекса «UFED»: Методические рекомендации./ Ю.М. Баркалов. – ВИ МВД России, 2015.