Банк России
Центральный банк Российской Федерации

1 ИЮНЯ 2016 –
1 СЕНТЯБРЯ 2017

ОТЧЕТ ЦЕНТРА МОНИТОРИНГА И РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ АТАКИ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ ГЛАВНОГО УПРАВЛЕНИЯ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ БАНКА РОССИИ

Москва

БАНК РОССИИ

ФИНЦЕРТ

Настоящий отчет подготовлен Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России) Главного управления безопасности и защиты информации Банка России.

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

AD (Active Directory)	Служба каталогов
ATM (Automated Teller Machine)	Банкомат
BIOS (Basic Input/Output System)	Базовая система ввода-вывода
DDoS	Распределенная атака типа «отказ в обслуживании» с одновременным использованием большого числа атакующих компьютеров, целью которой, как правило, является частичное нарушение штатного функционирования информационной инфраструктуры организации
Firewall	Межсетевой экран
PIN-код (Personal Identification Number)	Служит для авторизации держателя карты
PIN-пад	Устройство для ввода PIN-кода
RAT (Remote Access Tool)	Средство удаленного управления
SDC	Системная шина банкомата
TOR (The Onion Router)	«Луковая» маршрутизация
АРМ	Автоматизированное рабочее место
АРМ КБР	Автоматизированное рабочее место клиента Банка России
Ботнет	Компьютерная сеть, состоящая из узлов с запущенным однотипным централизованно управляемым вредоносным ПО
Ботнет-клиент	Зараженное устройство, которым может удаленно управлять злоумышленник
ВПО	Вредоносное программное обеспечение
ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
ДБО	Дистанционное банковское обслуживание
Командный сервер	Сервер, как правило в сети Интернет, с которого ведется управление зараженными устройствами
КО	Кредитная организация
ЛВС	Локальная вычислительная сеть
МЭ	Межсетевой экран
ОС	Операционная система
ПО	Программное обеспечение
ФинЦЕРТ	Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России

ВВЕДЕНИЕ

Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) – структурное подразделение Главного управления безопасности и защиты информации Банка России.

На сегодняшний день в штате ФинЦЕРТ насчитывается 28 квалифицированных работников, имеющих богатый практический опыт в области анализа защищенности и уязвимостей информационных систем, а также векторов атак, реализуемых на их основе. Работники ФинЦЕРТ имеют высшее техническое и экономическое образование (трое – ученую степень), полученное в таких высших учебных заведениях, как МГТУ им. Н.Э. Баумана, НИЯУ МИФИ и МГУ им. М.В. Ломоносова. У многих сотрудников есть опыт работы в банковской сфере и правоохранительных органах. Помимо этого, специалисты ФинЦЕРТ регулярно проходят курсы, направленные на повышение квалификации. Средний возраст составляет 34 года.

Основная цель функционирования ФинЦЕРТ – создание центра компетенции в рамках информационного взаимодействия Банка России, поднадзорных ему организаций, компаний-интеграторов, разработчиков ПО, в том числе средств антивирусной защиты, провайдеров и операторов связи, а также правоохранительных и иных государственных органов, курирующих информационную безопасность отрасли. Указанное информационное взаимодействие направлено на обмен информацией о потенциальных компьютерных атаках в кредитно-финансовой сфере, актуальных угрозах информационной безопасности и уязвимостях ПО, используемого организациями, поднадзорными Банку России. Результатом информационного взаимодействия является разработка рекомендаций и аналитических материалов в области обеспечения защиты информации при осуществлении переводов денежных средств на основе анализа данных о фактах компьютерных атак на организации, поднадзорные Банку России.

Для достижения указанных целей выполняются следующие задачи:

- *организация и координация обмена информацией между ФинЦЕРТ, организациями, поднадзорными Банку России, и правоохранительными органами (Министерство внутренних дел Российской Федерации, Федеральная служба безопасности Российской Федерации, ГосСОПКА);*
- *мониторинг открытых ресурсов сети Интернет для обнаружения и предупреждения информационных атак;*
- *проведение компьютерных исследований (форензика);*
- *дистанционный контроль защиты информации при осуществлении переводов денежных средств;*
- *участие в инспекционной деятельности Банка России.*

Настоящий отчет о деятельности ФинЦЕРТ охватывает второе полугодие 2016 года и первое полугодие 2017 года и предназначен для широкого круга заинтересованных лиц.

1. ОРГАНИЗАЦИЯ И КООРДИНАЦИЯ ОБМЕНА ИНФОРМАЦИЕЙ

1.1. Взаимодействие с организациями кредитно-финансовой сферы

Количество участников информационного обмена ФинЦЕРТ постоянно увеличивается. На рисунке 1 приведена динамика присоединения кредитных организаций к информационному обмену, начиная с предыдущего отчетного периода. По состоянию на 1 сентября 2017 года в информационном обмене участвовали 418 кредитных организаций и филиалов. Заметный рост числа участников – кредитных организаций наблюдался в январе – феврале 2017 года после серии рассылок злоумышленниками загрузчиков Cobalt Strike в адрес кредитных организаций.

Рисунок 1

Количество кредитных организаций, присоединившихся к информационному обмену с ФинЦЕРТ

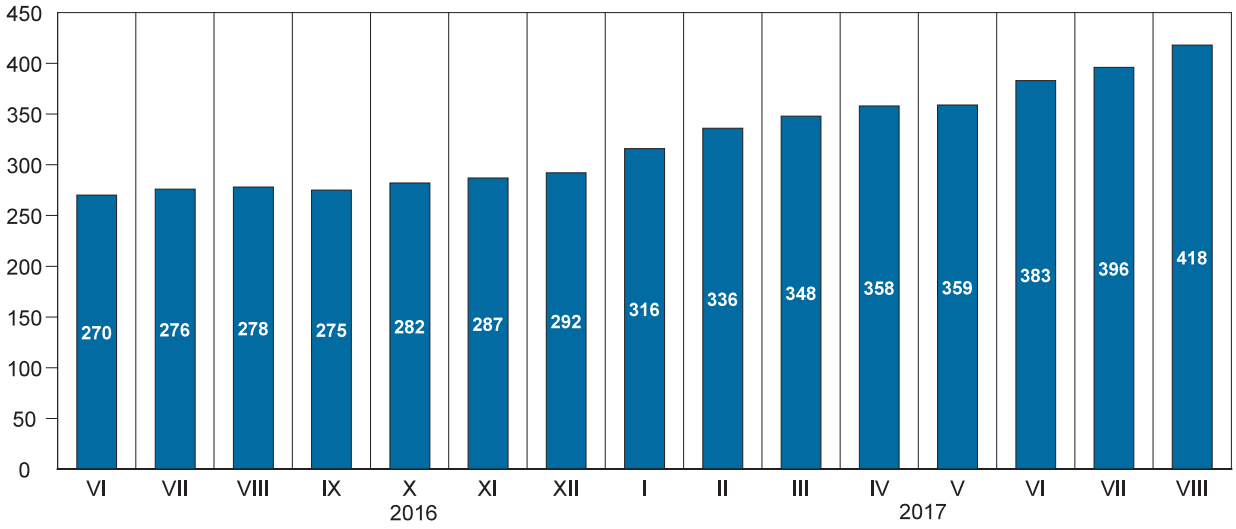


Рисунок 2

Общее число участников информационного обмена по типу организации

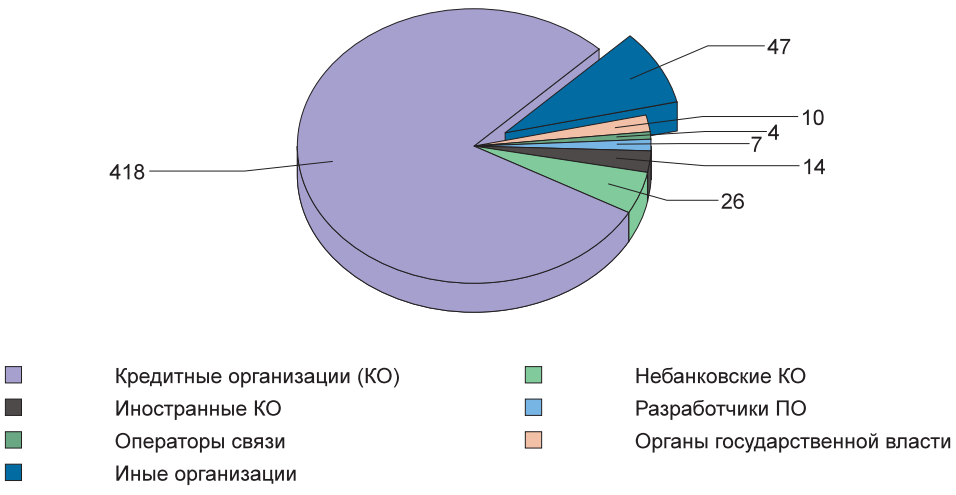
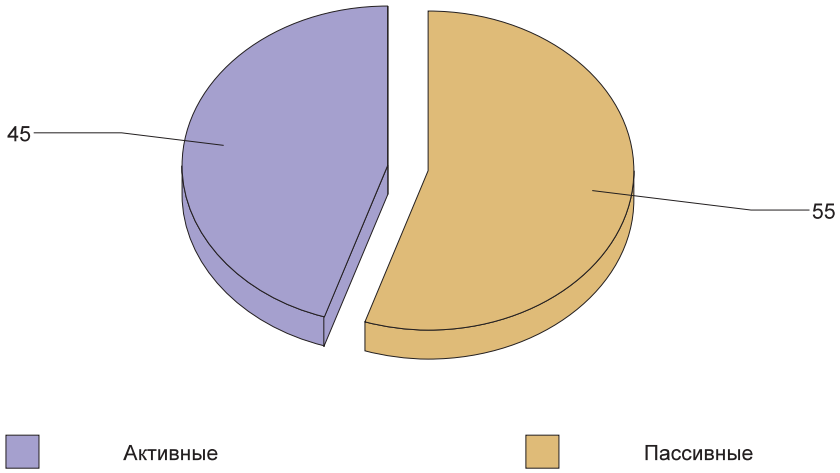


Рисунок 3

Доля активных участников информационного обмена (%)



Общее количество участников информационного обмена в разрезе их сферы деятельности приведено на рисунке 2. По сравнению с предыдущим отчетным периодом прирост количества участников составил 65%.

14 кредитных организаций из стран, входящих в ОДКБ (Организация Договора о коллективной безопасности), 26 небанковских кредитных организаций, 7 разработчиков банковского программного обеспечения, 4 оператора связи, 10 органов государственной власти и иные организации из разных сфер деятельности.

За данный отчетный период доля активных участников информационного обмена ФинЦЕРТ, которые регулярно передают информацию о выявленных угрозах и уязвимостях, увеличилась почти в два раза. Соотношение активных и пассивных участников информационного обмена представлено на рисунке 3.

Стоит отметить, что ФинЦЕРТ активно сотрудничает с правоохранительными органами: в ряде случаев работники ФинЦЕРТ привлекались в качестве экспертов при расследовании уголовных дел, связанных с хищениями денежных средств у кредитных организаций.

1.2. Реагирование на сообщения об атаках

Основная часть информации об атаках поступает в ФинЦЕРТ от участников информационного обмена (аналогичная тенденция наблюдалась и в предыдущем отчетном периоде). Распределение источников информации представлено на рисунке 4.

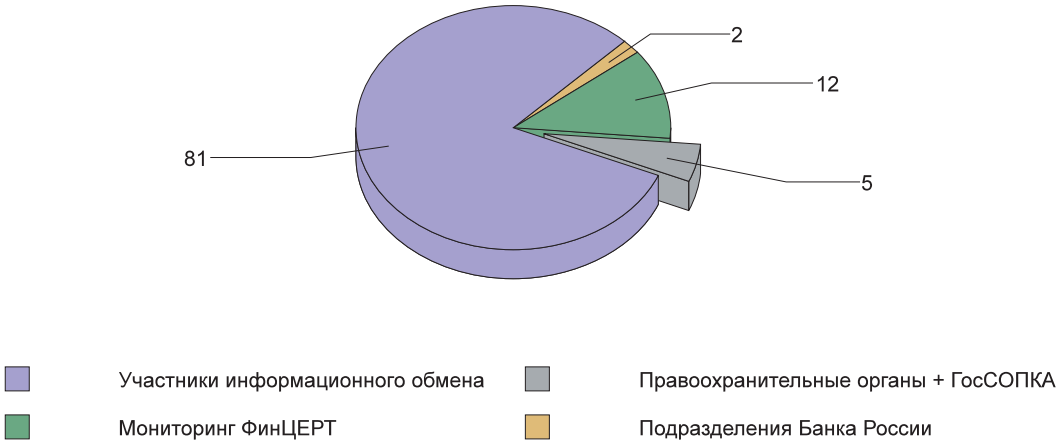
Получая от участника обмена сообщение об угрозе, ФинЦЕРТ проводит его анализ с помощью средств автоматизации или в ручном режиме, если требуется более детальное выявление индикаторов компрометации. После этого формируется и рассылается информационный бюллетень (в среднем за месяц ФинЦЕРТ выпускает около 14 бюллетеней). Статистика по количеству разосланных бюллетеней за отчетный период отражена на рисунке 5.

ФинЦЕРТ готовит и рассылает бюллетень в случаях получения одного и того же образца ВПО (или его модификаций) от нескольких участников информационного обмена либо в ситуациях, когда присланный образец ВПО несет собой большой риск для участников информационного обмена. Величина риска определяется по следующим критериям:

- подозрение на целевую атаку на организации, поднадзорные Банку России;
- массовость обращений участников информационного обмена в отношении образца ВПО и/или его модификаций (на сегодняшний день рассылка ВПО считается массовой при ее наличии у 10 и более участников информационного обмена);
- выявление нового образца ВПО для мобильных устройств и/или его модифика-

Рисунок 4

Распределение источников получения информации (%)



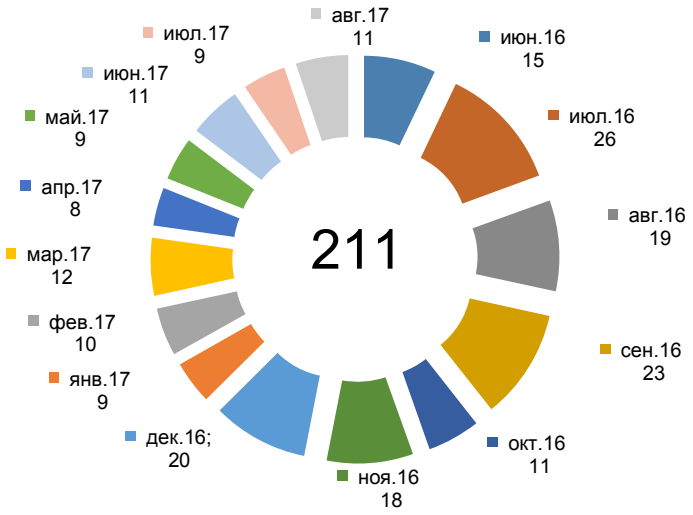
ций, направленных на хищение средств у клиентов кредитных организаций;

- показатель выявления на VirusTotal составляет менее 5 антивирусных средств или отсутствие детектирования распространенными в России антивирусными средствами. Данный показатель имеет средний приоритет: скорость обновления баз VirusTotal зачастую ниже, чем у непосредственных клиентов антивирусных компаний. В случаях, когда на VirusTotal образец не детектируется, он дополнительно отправляется в антивирусные лаборатории, участвующие в обмене.

В ситуации когда участник обмена сообщает об атаке, по которой бюллетень уже разослан, и ФинЦЕРТ не находит новых индикаторов компрометации (IOC), то повторно бюллетень не рассылается. В таком случае с участником проводится индивидуальная консультация. При обнаружении новых IOC выпускается обновленный бюллетень со ссылкой на предыдущий.

Рисунок 5

Количество бюллетеней, рассылаемых ФинЦЕРТ, в разрезе по месяцам



1.3. Подготовка предложений по разделегированию доменов в сети Интернет

ФинЦЕРТ уведомляет регистраторов доменных имен о доменах, с которых рассылается вредоносный код и осуществляются мошеннические действия, связанные с использованием платежных карт. Основные критерии, по которым в отношении домена могут быть подготовлены предложения по разделегированию:

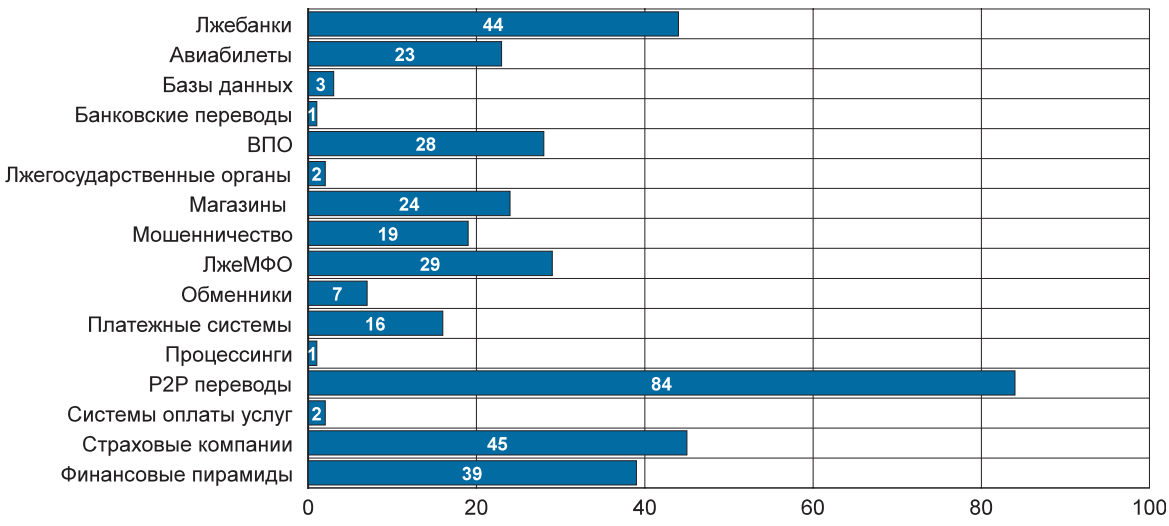
- с домена рассылается вредоносный код (срабатывание антивируса, анализ ФинЦЕРТ, подтверждение от компетентной организации);
- на домене находится сайт, собирающий данные платежных карт (имя владельца, номер, срок действия, код подлинности карты);
- на домене находится сайт, имитирующий ресурсы Банка России;
- домен является командным центром ботнет-сети (данные Threat Intelligence, информация, полученная от участников информационного обмена, правоохранительных органов);
- на домене находится сайт с материалами фишингового содержания в отношении клиентов организаций кредитно-финансовой сферы;
- домен используется как площадка, на которой широко представлены темы, посвященные мошенничеству в финансовой сфере и продажам дампов (копий) карт.

В рамках указанной деятельности ФинЦЕРТ взаимодействует с:

- координационным центром Национального домена сети Интернет (зоны .RU, .РФ);
- фондом развития Интернет (зона .SU);
- MSK-IX (зоны .PP.RU, .NET.RU, ORG.RU);
- фондом содействия развитию технологий и инфраструктуры сети Интернет (зоны COM.RU, EXNET.SU, RU.NET, а также «геодомены»: .ABKHAZIA.SU, .ADYGEYA.RU, .ADYGEYA.SU, .AKTYUBINSK.SU, .ARKHANGELSK.SU, .ARMENIA.SU, .ASHGABAD.SU, .AZERBAI-JAN.SU, .BALASHOV.SU, .BASHKIRIA.RU, .BASHKIRIA.SU, .BIR.RU, .BRYANSK.SU, .BUKHARA.SU, .CBG.RU, .CHIMKENT.SU, .COM.RU, .DAGESTAN.RU, .DAGESTAN.SU, .EAST-KAZAKHSTAN.SU, .GEORGIA.SU, .GROZNY.RU, .GROZNY.SU, .IVANOVO.SU, .KALMYKIA.RU, .JAMBYL.SU, .KAL-MYKIA.SU, .KALUGA.SU, .KARA-COL.SU, .KARAGANDA.SU, .KARELIA.SU, .KHAKASSIA.SU, .KRASNODAR.SU, .KURGAN.SU, .KUSTANAI.RU, .KUSTANAI.SU, .LENUG.SU, .MANGYSHLAK.SU, .MA-RINE.RU, .MORDOVIA.RU, .MORDOVIA.SU, .MSK.RU, .MSK.SU, .MURMANSK.SU, .MYTIS.

Рисунок 6

Статистика по типу разделегированных доменов



RU, .NALCHIK.RU, .NALCHIK.SU, .NAVOI.SU, .NORTH-KAZAKHSTAN.SU, .NOV.RU, .NOV.SU, .OBNINSK.SU, .PENZA.SU, .POKROVSK.SU, .PYATIGORSK.RU, .SOCHI.SU, .SPB.RU, .SPB.SU, .TASHKENT.SU, .TERMEZ.SU, .TOGLIATTI.SU, .TROITSK.SU, .TSELINOGRAD.SU, .TULA.SU, .TUVA.SU, .VLADIKAVKAZ.RU, .VLADIKAVKAZ.SU, .VLADIMIR.RU, .VLADIMIR.SU и .VOLOGDA.SU).

Этапы процесса при подготовке предложений по разделегированию доменов в сети Интернет:

1) получение запроса на разделегирование;

2) анализ на предмет наличия признаков мошеннической деятельности;

3) при обнаружении признаков мошеннической деятельности ФинЦЕРТ уведомляет регистратора о целесообразности снятия домена с делегирования или инициирования проверки документов его администратора;

4) в случае, если оцениваемый домен лежит вне компетенции ФинЦЕРТ, полученные сведения направляются на рассмотрение иным компетентным организациям;

5) уведомление лица, приславшего сайт на рассмотрение ФинЦЕРТ, о передаче регистратору информации о целесообразности принятия соответствующих мер;

6) получение ответа от регистратора;

7) уведомление лица, приславшего сайт на рассмотрение ФинЦЕРТ, о решении регистратора (приостановление делегирования, снятие с делегирования, отсутствие оснований для снятия с делегирования).

Среднее время разделегирования доменов занимает от 1 до 3 дней.

С 1 января 2017 года по 1 сентября 2017 года ФинЦЕРТ отправил информацию о 481 домене различной мошеннической тематики, подлежащем разделегированию (367 доменов по итогам рассмотрения заблокированы регистраторами). В среднем за месяц разделегированию подлежат около 50 доменов, находящихся в различных зонах.

Статистика по типу разделегированных доменов представлена на рисунке 6.

2. МОНИТОРИНГ ОТКРЫТЫХ РЕСУРСОВ СЕТИ ИНТЕРНЕТ ДЛЯ ОБНАРУЖЕНИЯ И ПРЕДУПРЕЖДЕНИЯ ИНФОРМАЦИОННЫХ АТАК

ФинЦЕРТ на постоянной основе проводит мониторинг открытых ресурсов сети Интернет для обнаружения и предупреждения информационных атак.

В течение рабочего дня с интервалом примерно в два часа ФинЦЕРТ осуществляет мониторинг СМИ, блогов, социальных сетей и аналогичных ресурсов сети Интернет на наличие публикаций, порочащих репутацию кредитных организаций.

При обнаружении сообщений дестабилизационного или негативного характера проводится мониторинг ресурсов сети Интернет по заданным параметрам с помощью поисковых систем и социальных медиа, чтобы выявить первоисточник перепечатанных сообщений. Одновременно с этим уведомляется потерпевшая кредитная организация.

Типовая информационная атака развивается, как правило, по следующему сценарию:

1. Появление первых публикаций в небольшом количестве, порочащих репутацию КО.

2. По прошествии некоторого времени обнаруживается масштабное количество ссылок и перепечаток как обычными пользователями, так и атакующими, в полном или частичном виде в социальных сетях ВКонтакте, Facebook, Twitter (в среднем от 200 до 800 перепечаток в сутки). В некоторых случаях отмечается кампания в популярных мессенджерах: Viber, Telegram, WhatsApp.

3. ФинЦЕРТ анализирует и готовит необходимые справки, которые передаются в соответствующие подразделения для принятия решений. Чаще всего мониторинг происходит с помощью автоматизированных инструментов.

4. После значительного снижения количества перепечаток в сутки относительно предыдущих дней отслеживание данной тематики прекращается.

3. ПРОВЕДЕНИЕ КОМПЬЮТЕРНЫХ ИССЛЕДОВАНИЙ (ФОРЕНЗИКА)

3.1. Основные задачи

К основным задачам ФинЦЕРТ в рамках проведения компьютерных исследований относятся:

- анализ поступающего от участников информационного обмена ВПО и подозрительных URL-ссылок;
- выработка мер противодействия и выявление индикаторов компрометации (IOC).

На сегодняшний день у ФинЦЕРТ есть возможность проводить исследования носителей информации, мобильных и других радиоэлектронных устройств.

Начиная с декабря 2016 года ФинЦЕРТ проводит компьютерные криминалистические исследования в интересах правоохранительных органов. За отчетный период проведено шесть исследований электронных носителей информации, подвергшихся воздействию ВПО при совершении хищений денежных средств со счетов клиентов кредитных организаций; три исследования аппаратных средств, предназначенных для скрытого хищения платежной информации, а также несколько исследований различных мобильных устройств и поддельных платежных карт.

3.2. Основные типы фиксируемых атак

За отчетный период были обнаружены следующие основные типы атак:

- DDoS-атаки, в том числе угрозы DDoS-атак;
- массовые рассылки почтовых сообщений, содержащих загрузчики ВПО (атаки с элементами социальной инженерии);
- атаки, направленные на устройства самообслуживания.

3.3. Динамика атак

На рисунке 7 представлена статистика по типам атак, зарегистрированных ФинЦЕРТ.

Динамика мощности DDoS-атак приведена на рисунке 8.

Рисунок 7

Динамика основных типов атак (по кварталам)

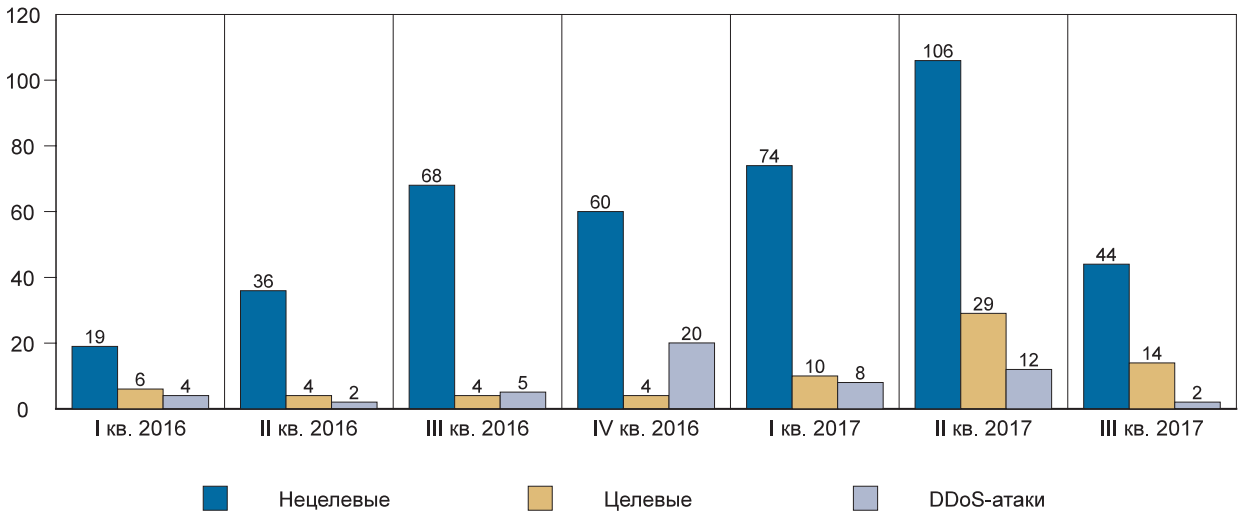
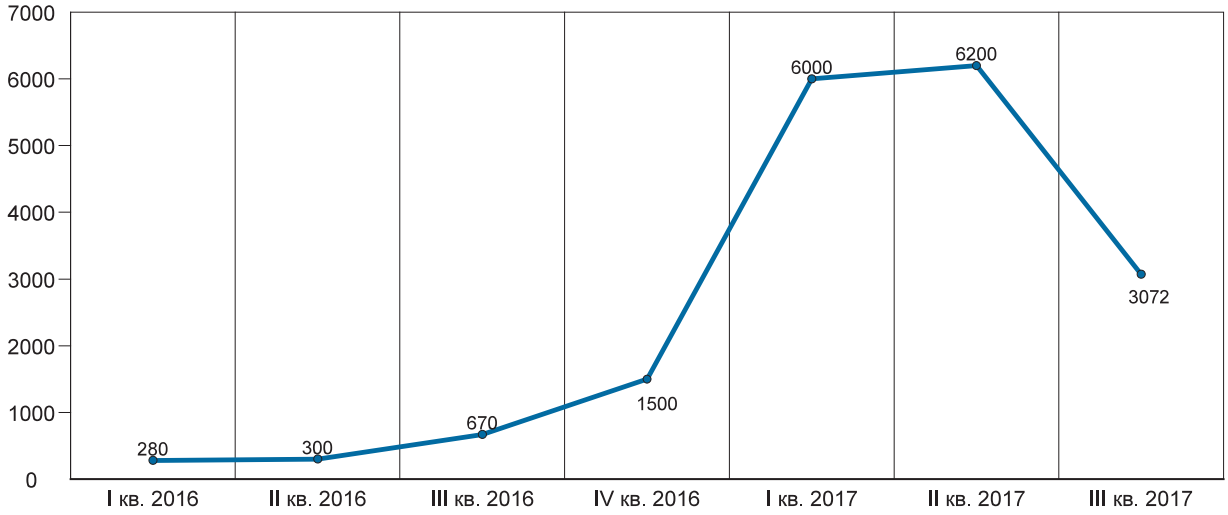


Рисунок 8

Статистика по мощности DDoS-атак (Мбит/с)



3.4. Массовые рассылки почтовых сообщений, содержащих загрузчики ВПО (атаки, имеющие отношение к социальной инженерии)

Процентное соотношение типов вложений фишинговых писем приведено на рисунке 9.

По мнению ФинЦЕРТ, существует несколько источников, из которых формируются базы данных по кредитным организациям для последующей рассылки:

- утечка почтовых адресов из регистрационных баз различных конференций. Подобные базы данных продаются достаточно недорого на специализированных форумах, а в некоторых случаях раздаются бесплатно;
- поиск в сети Интернет через специализированные ресурсы;
- документы и веб-страницы кредитных организаций, содержащие почтовые адреса сотрудников организаций, общедоступные адреса (например, таких как info@companyname);

Рисунок 9

Процентное соотношение типов вложений в 2017 году (%)

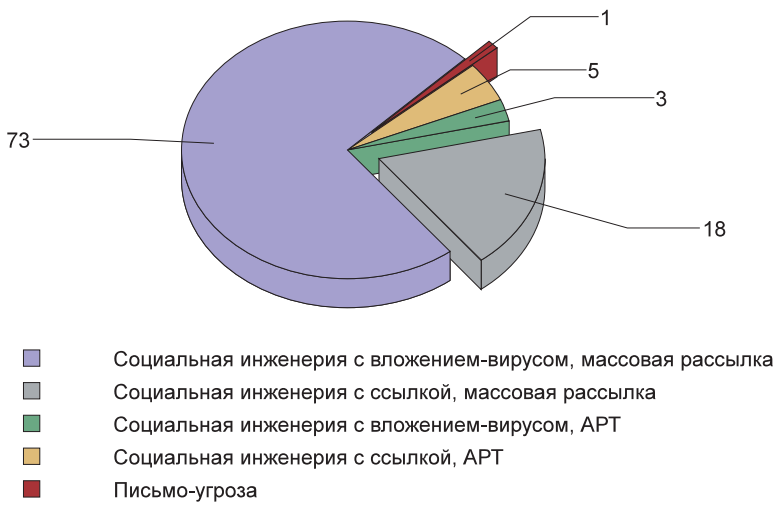


Рисунок 10

Пример сообщения о продаже базы данных банковских работников

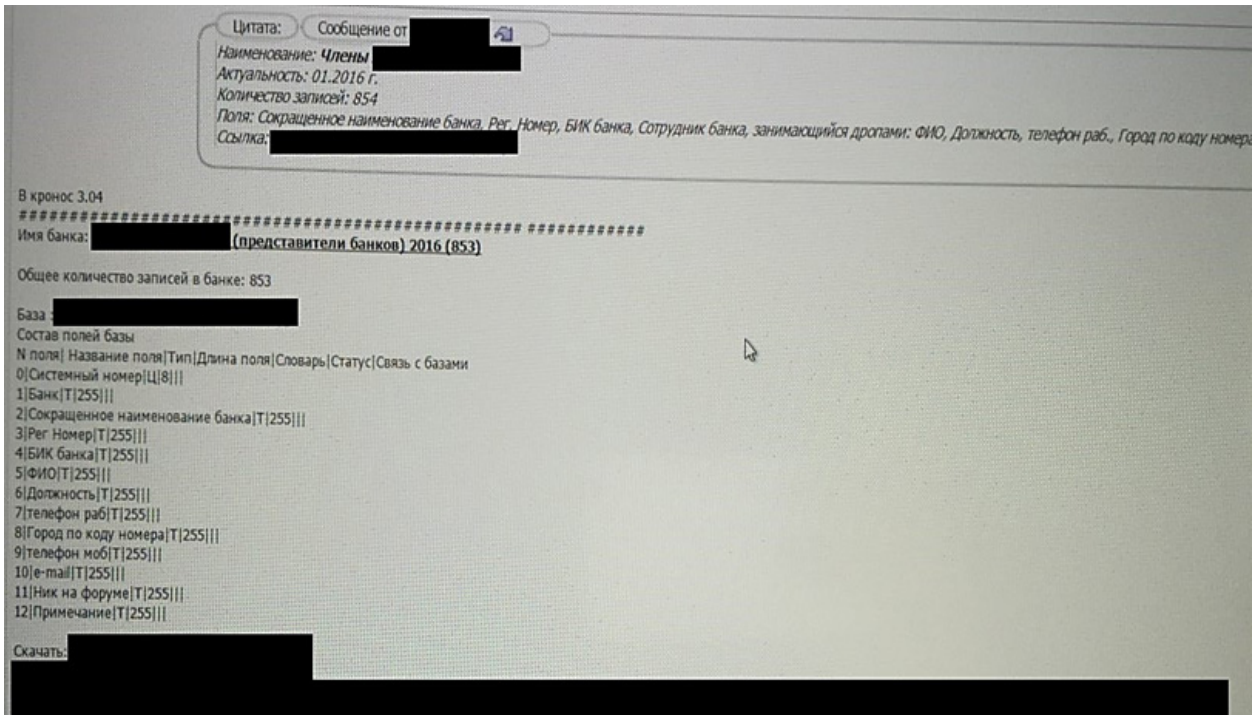
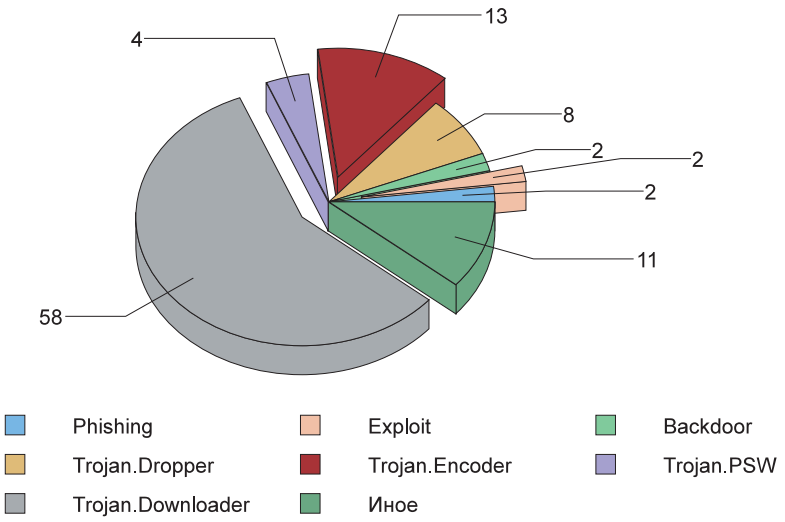


Рисунок 11

Типы вредоносного программного обеспечения (%)



- утечки баз данных (списков рассылок) различных неформальных сообществ, объединенных по профессиональному признаку.

Наиболее эффективным способом борьбы со спамом можно считать наличие в организации специализированных решений по проверке почты (Email Gateway) и оперативное добавление адресатов в списки нежелательных отправителей на почтовом шлюзе.

Статистика по типам ВПО, которое содержится в фишинговых письмах, как целевых, так и общей направленности, представлена на рисунке 11.

Наибольшее количество рассылок (58%) приходится на вредоносные программы типа Trojan.Downloader: по сравнению с предыдущим отчетным периодом доля подобных вложений увеличилась на 5%.

Trojan.Downloader – вредоносная программа, главная цель которой – загрузка и установка на компьютер различных вредоносных и «троянских» программ. Такого рода программы содержат в себе заранее прописанные имена и расположение файлов, скачиваемых загрузчиком с управляющего сервера. Зачастую загруженные вредоносные программы прописываются «троянской» программой в автозагрузке.

Trojan.Encoder – вредоносная программа, шифрующая файлы на жестком диске компьютера и требующая деньги за их расшифровку. В результате зашифрованными могут оказаться файлы *.doc, *.docx, *.pdf, *.jpg, *.rar и так далее. Доля таких вложений составила 13%, что на 5% меньше, чем в предыдущем отчетном периоде. Вероятно, это связано с более качественным обнаружением подобного рода писем и их фильтрацией, из-за чего они не доходят до конечного получателя.

Backdoor – вредоносная программа, назначение которой – скрытое от пользователя удаленное управление злоумышленником компьютером жертвы (фактически по функционалу это программа удаленного администрирования). Часто такие программы используются для создания ботнетов. Доля подобных вложений составила 2%, что на 8% меньше по сравнению с предыдущим отчетным периодом. Это может объясняться тем, что данное ВПО устанавливается после успешного запуска Trojan.Downloader или Trojan.Dropper.

Exploit – вредоносная программа, содержимое которой (некоторые данные, исполняемый код) позволяет использовать имеющиеся уязвимости в ПО, установленном на компьютере.

Полученные ФинЦЕРТ образцы таких программ использовали уязвимости, которые можно было закрыть обновлением программного обеспечения или установкой патча. Доля подобного ВПО составила 2%, что на 4% меньше, чем в предыдущем отчетном периоде. Это объясняется еще и тем, что данное ВПО устанавливается после успешного запуска Trojan.Downloader или Trojan.Dropper.

Trojan.Dropper – вредоносная программа, предназначенная для установки на компьютер содержащихся в теле «троянской» программы других вредоносных программ. Обычно установка вредоносных программ происходит без разрешения пользователя и скрытно от него. В некоторых случаях пользователю приходят ложные сообщения об ошибке в архиве, в программе при открытии файла и так далее. Чаще всего вредоносные программы типа Trojan.Dropper сохраняются в каталоги Windows, в том числе системные или временные каталоги. Доля случаев распространения подобного рода ВПО увеличилась вдвое по сравнению с предыдущим отчетным периодом и составила 8%.

Trojan.PSW – класс вредоносных программ, предназначенных для кражи пользовательских авторизационных данных (логин и пароль, в некоторых случаях – сертификаты пользователей). В предыдущем отчетном периоде доля подобных программ была невелика и отнесена в раздел «иное». В последнее время активность таких программ возросла, составив 4%, что позволило вынести их в отдельную категорию.

Phishing – мошеннические письма с отсутствующими вредоносными вложениями, но содержащие различные ссылки, по которым предлагается перейти пользователю. В текущем отчетном периоде доля Phishing составила 4% от общего количества проанализированных ФинЦЕРТ объектов, что на 2%меньше, чем в предыдущем отчетном периоде.

3.5. Атаки на устройства самообслуживания

В отчетный период вырос интерес злоумышленников к атакам на устройства самообслуживания (далее – АТМ или банкоматы). ФинЦЕРТ разделяет атаки на устройства самообслуживания на два основных типа:

- логические атаки (устройство не повреждается или не вскрывается, не устанавливаются дополнительные аппаратные компоненты с подключением к шинам устройства, все операции выполняются через удаленный доступ с использованием программных средств);
- физические атаки (повреждение или вскрытие устройства, установка дополнительных аппаратных компонентов, под-

ключение внешних устройств, в том числе для возможности удаленного управления).

Вне зависимости от типа атаки все из них, за исключением подмены процессинга, направлены на опустошение диспенсера банкомата путем генерации соответствующих команд, якобы полученных от процессинга, с нарушением логики работы устройства

3.5.1. Логические атаки

Основной тренд логических атак во второй половине 2016 года и первой половине 2017 года – использование ПО Cobalt Strike, изначально предназначенного для проведения тестирования на проникновение. В данном случае Cobalt Strike – средство для получения удаленного доступа к банкоматам и передачи на них ПО, непосредственно взаимодействующего с XFS-фреймворком банкомата для выдачи денежных средств. После выдачи денежных средств, как правило, запускаются программы для уничтожения информации наподобие SDelete – легальной утилиты по уничтожению файлов от Microsoft. Данная атака подробно описана в приложении 3.

Часто встречается использование модифицированных инженерных программ, позволяющих провести выдачу наличных денежных средств из диспенсера. Помимо этого, существует отдельный класс программ, которые эксплуатируют особенности XFS и взаимодействуют с устройствами банкомата. Как правило, нет универсальных программ – они разработаны под конкретного производителя (NCR, Wincor, Diebold).

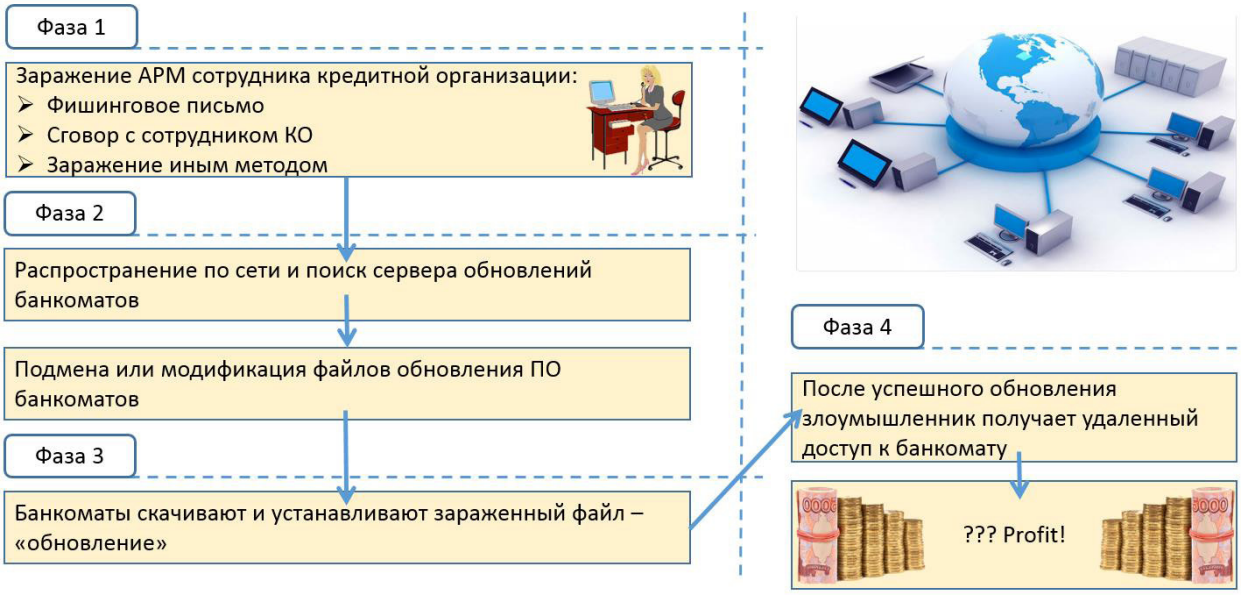
В середине 2016 года была зарегистрирована атака, подменяющая содержимое на сервере обновлений (замена или модифицирование легального файла обновлений для возможности получения удаленного доступа к банкомату либо внедрения вредоносной программы), с которого автоматически скачивались и устанавливались обновления банкомата. Общая схема атаки представлена на рисунке 12.

Чтобы атака была успешной, злоумышленнику необходимо:

- Закрепиться в сети кредитной организации. Для этого часто используются приемы социальной инженерии, рассылка фишинговых писем. Во вложенных документах могут как эксплуатироваться уязвимости MS Office, так и содержаться скрипты.
- Выполнить поиск сервера обновления банкомата. Для этого прибегают к сканированию сети и взлому сервера контроллера доменов для получения сведений о структуре сети и учетных записей (может использоваться также информация из файла

Рисунок 12

Схема атаки с подменой обновлений



Groups.xml, описанного в разделе о Cobalt Strike).

- После нахождения сервера обновлений и получения к нему доступа атакующий пытается подменить файлы обновлений или создать ложное внеочередное обновление. Если это удается, то он получает контроль над всей сетью банкоматов организации, на которую поступают обновления с конкретного сервера. Чаще всего это удаленный доступ к банкоматам и возможность загружать на него свои приложения.
- После успешного получения доступа к банкоматам в определенное время к нему подходят «нальщики» («дропы», «мулы») и по команде оператора получают наличные денежные средства.

Основные факторы успешности атаки:

- чаще всего все файлы, полученные с сервера обновления, считаются доверенными, и им позволено выполняться с административными привилегиями;
- как следствие, возможно внесение атакующим модифицированных системных файлов, добавление новых файлов с занесением их в «белый список» контроля запуска приложений.

Возможные меры противодействия атаке:

- Недопущение нахождения АРМ сотрудника с возможностью получения внешней почты в одном сегменте сети с сервером обновления банкоматов.
- Повышение осведомленности сотрудников.
- Эксплуатация на критических АРМ альтернативных редакторов документов Office, не подверженных уязвимостям оригинального редактора.
- Использование только подписанных обновлений, исключение возможности установки неподписанных обновлений.

Контроль доступа к серверу обновления банкоматов осуществляется по протоколам RPC, SMB.

По состоянию на 1 сентября 2017 года ФинЦЕРТ известны по меньшей мере два факта атак описанным методом.

3.5.2. Физические атаки

Основные категории «физических» атак остались традиционными.

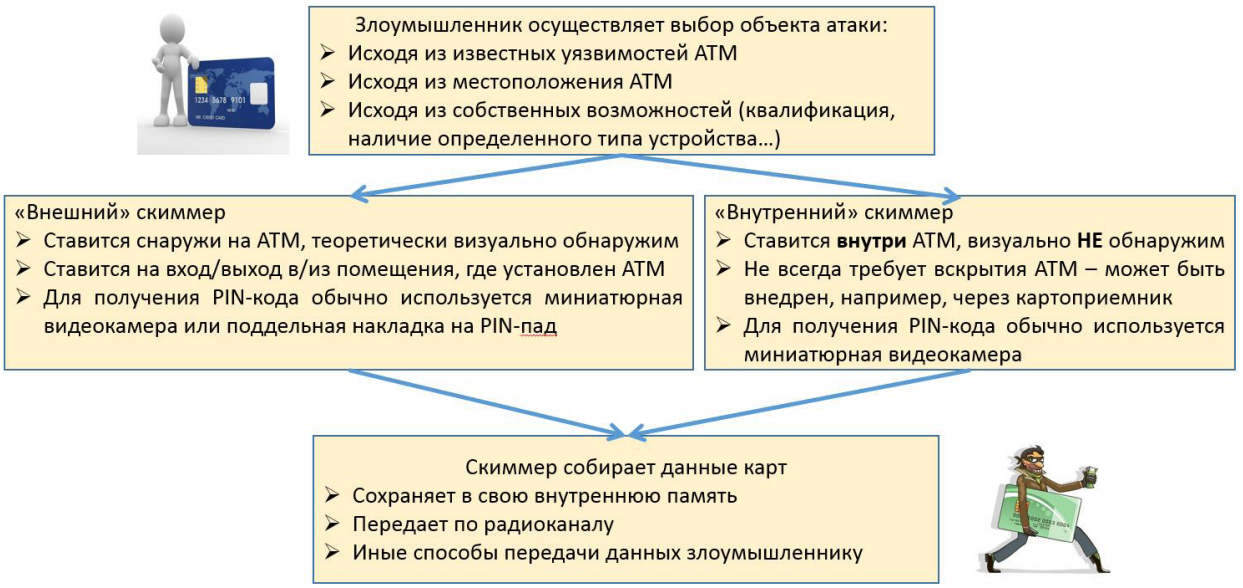
Скимминг. Установка специальных технических средств, причем не обязательно в картоприемник, для хищения данных, записанных на магнитную ленту платежной карты. PIN-код, как правило, похищается с помощью отдельного технического устройства – видеокамеры или фальшивой накладки на PIN-пад. Примеры скиммингового оборудования представлены на рисунке 13. В отдельных случаях злоумышленники могут изготавливать скимминговое оборудование под конкретного заказ-

Рисунок 13

Примеры скиммингового оборудования (данные получены с ресурса, продающего скимминговое оборудование)

Рисунок 14

Обобщенные данные по типам скимминговых атак



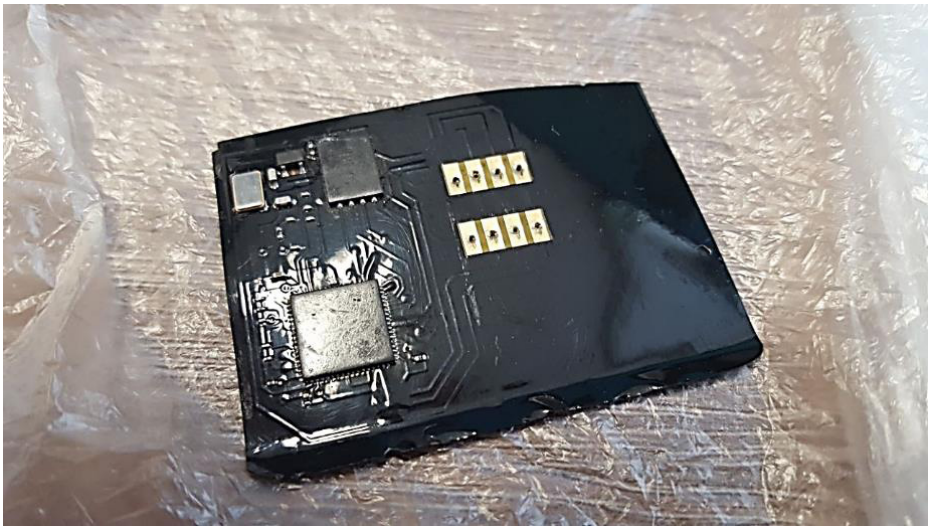
чика. В ряде случаев отмечено использование нового вида скимминговых оборудования – так называемого перископного. Факт появления новых видов скимминга доказывает, что криминальное сообщество постоянно работает над совершенствованием скимминговых устройств, не чувствительных к современным антискимминговым мерам.

На рисунке 14 приведены обобщенные данные по типам скимминговых атак.

Шимминг. Установка в картоприемник специальных технических средств, предназначенных для хищения данных с EMV-чипа карты (пример шиммера представлен на рисунке 15). Таким образом похищается следующая информация: история платежей, информация, содержащаяся на Track 2 карты, срок действия. Следует отметить, что для платежных карт, эмитированных российскими банками, данное оборудование практически бесполезно – провести операцию по дубликату чипа карты, выпущенной российским эмитентом, в подавляющем большинстве случаев невозможно. На момент составления отчета не зафиксировано успешных операций с использованием дубликата чипов российских эмитентов.

Рисунок 15

Шиммер, устанавливаемый в POS-терминал



Black Box. Установка либо подключение технического устройства, взаимодействующего с компонентами банкомата (чаще всего с диспенсером) и отдающего последнему команду для выдачи денежных средств. За отчетный период чаще всего встречалась разновидность атаки Black Box, связанная с подключением к SDC-шине банкомата (интерфейс передачи данных RS-485). В ряде случаев проводилось высверливание корпуса банкомата с подключением устройства к нему. При этом подключенное устройство пыталось выступить в качестве

Рисунок 16

Пример попытки атаки Black Box (удаление основного Master-устройства)

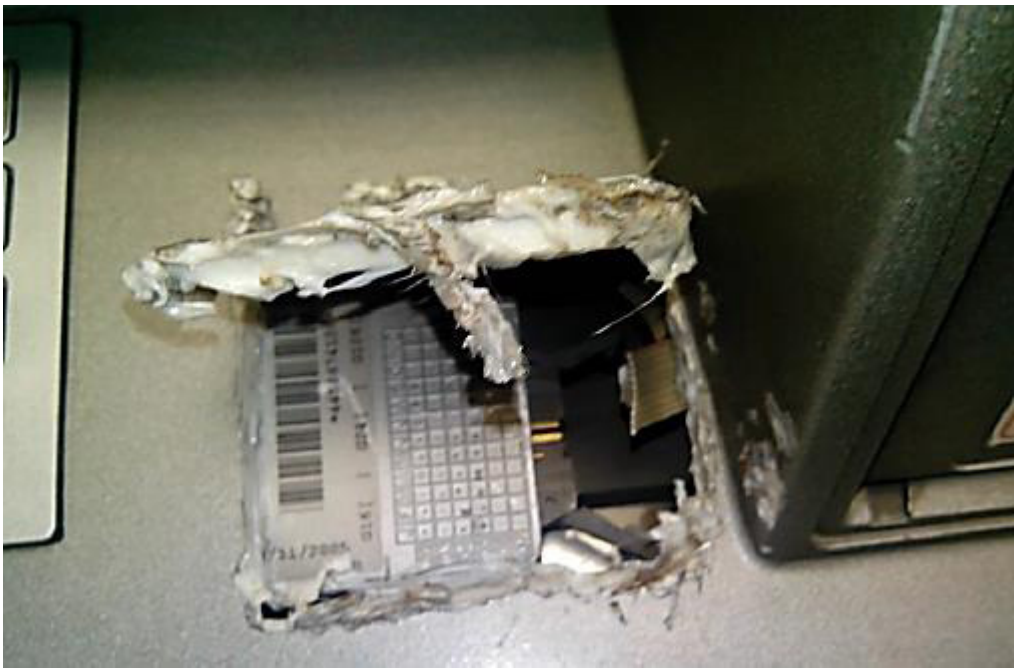


Рисунок 17

Пример устройства Black Box, подключаемого к разъему SDC и переносному ПК по интерфейсу USB. В данном случае, основные компоненты Black Box были реализованы в виде компьютерной программы

ведущего (Master) устройства. В результате такой атаки возникает конфликт устройств, требующий отключения одного ведущего (Master) устройства. Способы отключения основного (легального) Master-устройства различны и связаны с конкретными особенностями атакуемого банкомата. Пример неудачной атаки Black Box представлен на рисунке 16. Один из видов оборудования Black Box проиллюстрирован на рисунке 17.

Атаки на бесконтактные карты (NFC). Несмотря на отсутствие подтвержденных сведений о фактах успешного создания в России дубликатов платежных карт, существует техническая возможность хищения бесконтактным методом таких данных, как:

- тип используемого платежного приложения;
- срок действия карты;
- имя держателя карты;
- PAN (Primary Account Number) карты;
- история операций;
- количество оставшихся попыток ввода PIN-кода;
- другие данные, в том числе возможно отдельное хищение Track 2 магнитной полосы платежной карты.

Подмена процессинга. В этом случае банкомат отключается от процессинга кредитной организации и подключается к устройству, имитирующему его. Передовые устройства могут эмулировать нормальное состояние банкомата (обслуживание клиентов) для мониторинга ПО. Так, суть атаки заключается в передаче банкомату подложных команд о выдаче денежных средств без нарушения общей логики работы банкомата и модификации его компонентов, как аппаратных, так и программных.

Transaction Reversal Fraud (TRF). Цель данной атаки – получение наличных денежных средств с одновременным воздействием на работу банкомата и процессингового центра, в результате чего отсутствует корректное завершение операции по выдаче наличных средств и не меняется баланс по карте (манипулирование карточным счетом). Такая атака встречается крайне редко, но тем не менее она была зафиксирована в феврале 2017 года в Москве. Общий механизм в данном случае следующий: используется легальная EMV-карта, оснащенная специальной микросхемой – чипом:

1. Злоумышленники вставляют карту в банкомат и выбирают размер суммы для выдачи.

2. Банкомат подготавливает необходимую сумму, но еще не выдает ее («pre-present cash»), после чего банкомат возвращает карту.

3. По стандартному алгоритму работы злоумышленники не забирают карту, а удерживают ее, чтобы не допустить ее изъятия банкоматом (через 30–50 секунд банкомат изымает карту), или же подменяют ее любой другой картой. Пока злоумышленники с помощью отвертки или другого инструмента открывают шторку шаттера диспенсера и забирают Pre-Presented Cash, ПО банкомата генерирует ошибку из-за невозможности изъятия платежной карты и отправляет ее в процессинг (хост).

4. Хост инициирует операцию возврата (Reversal) на ранее списанную сумму. В итоге баланс карты не меняется.

5. Все повторяется заново при условии отсутствия повреждения механических частей шаттера.

На текущий момент ФинЦЕРТ не обладает собственной статистикой по атакам на устройства самообслуживания.

ЗАКЛЮЧЕНИЕ

Основная цель функционирования ФинЦЕРТ – создание центра компетенции в рамках информационного взаимодействия Банка России, поднадзорных ему организаций, компаний-интеграторов, разработчиков ПО, в том числе средств антивирусной защиты, провайдеров и операторов связи, а также правоохранительных и иных государственных органов, курирующих информационную безопасность отрасли. Указанное информационное взаимодействие направлено на обмен информацией о потенциальных компьютерных атаках в кредитно-финансовой сфере, актуальных угрозах информационной безопасности и уязвимостях ПО, используемого организациями, поднадзорными Банку России. Результатом информационного взаимодействия является разработка рекомендаций и аналитических материалов в области обеспечения защиты информации при осуществлении переводов денежных средств на основе анализа данных о фактах компьютерных атак на организации, поднадзорные Банку России.

Для достижения указанных целей выполняются следующие задачи:

- Организация и координация обмена информацией между ФинЦЕРТ, организациями, поднадзорными Банку России, и правоохранительными органами (Министерство внутренних дел Российской Федерации, Федеральная служба безопасности Российской Федерации, ГосСОПКА).
- Мониторинг открытых ресурсов сети Интернет для обнаружения и предупреждения информационных атак.
- Проведение компьютерных исследований (форензика).
- Дистанционный контроль защиты информации при осуществлении переводов денежных средств.
- Участие в инспекционной деятельности Банка России.

По состоянию на 1 сентября 2017 года в информационном обмене участвовали 418 кредитные организации и филиала. По сравнению с предыдущим отчетным периодом прирост количества участников составил 65%. ФинЦЕРТ активно сотрудничает с правоохранительными органами. В ряде случаев работники ФинЦЕРТ привлекались правоохранительными органами в качестве экспертов при расследовании уголовных дел, связанных с хищениями денежных средств у кредитных организаций.

В среднем в месяц рассылается около 14 бюллетеней.

С 1 января 2017 года по 1 сентября 2017 года ФинЦЕРТ отправил информацию о 481 домене различной мошеннической тематики, подлежащем разделегированию (367 доменов по итогам рассмотрения заблокированы регистраторами). В среднем за месяц разделегированию подлежат около 50 доменов, находящихся в различных зонах.

ФинЦЕРТ проводит на постоянной основе мониторинг открытых ресурсов сети Интернет для обнаружения и предупреждения информационных атак. В течение рабочего дня с интервалом примерно в 2 часа ФинЦЕРТ осуществляет мониторинг СМИ, блогов, социальных сетей и аналогичных ресурсов сети Интернет на наличие публикаций, порочащих репутацию руководства Банка России, банковских организаций.

За отчетный период были зафиксированы следующие основные типы атак:

- DDoS-атаки, в том числе угрозы DDoS-атак. Зафиксированная мощность атак возросла в 10 раз по сравнению с началом 2016 г. и составила 6200 Мбит/с.
- Массовые рассылки почтовых сообщений, содержащих загрузчики ВПО (атаки, имеющие отношение к социальной инженерии).
- Атаки, направленные на устройства самообслуживания.

На сегодняшний день основными инструментами дистанционного контроля являются анализ:

- сведений форм отчетности 0403203 и 0409258;
- обращений граждан;
- результатов оценки соответствия, проводимой субъектами национальной платежной системы в рамках выполнения требований Положения Банка России № 382-П;
- правил платежных систем на соответствие требованиям, касающимся обеспечения защиты информации при осуществлении переводов денежных средств в платежной системе.

С начала 2017 года ФинЦЕРТ участвует в инспекционной деятельности Банка России. Так, с начала 2017 года проверено семь банков, четыре страховые организации и одна расчетная небанковская кредитная организация.