Банк России

Центральный банк Российской Федерации

Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России

За период с 01 июня 2015 г. по 31 мая 2016 г.

Оглавление

1. Термины и определения 3
2. Введение 4
3. Основные показатели деятельности FinCERT 4
4. Основные типы атак, зафиксированные FinCERT 7
4.1. Целенаправленные атаки, связанные с подменой входных данных для АРМ КБР 7
4.1.1. Статистика по атакам, связанным с подменой входных данных для АРМ КБР 8
4.1.2. Технические сведения по атакам, связанным с подменой входных данных для АРМ КБР 8
4.1.3. Общие меры по противодействию атакам, связанным с подменой входных данных для АРМ КБР 9
4.2. Рассылки электронных сообщений, содержащих вредоносное ПО 9
4.2.1. Статистика по рассылкам электронных сообщений, содержащих вредоносное ПО 11
4.2.2. Технические сведения по рассылкам электронных сообщений, содержащих вредоносное ПО 12
4.2.3. Общие меры по противодействию 13
4.3. Атаки, направленные на устройства самообслуживания 13
4.3.1. Статистика по атакам, направленным на банкоматы 13
4.3.2. Технические сведения по атакам, направленным на банкоматы 14
4.3.3. Общие меры по противодействию атакам, направленным на банкоматы 14
4.3.4. Статистика по атакам, направленным на POS-терминалы 15
4.3.5. Технические сведения по атакам, направленным на POS-терминалы 15
4.3.6. Общие меры по противодействию атакам, направленным на POS-терминалы 16
4.4. DDoS-атаки 16
4.4.1. Статистика по DDoS-атакам 17
4.4.2. Технические сведения по DDoS-атакам 17
4.4.3. Общие меры по противодействию DDoS-атакам 18
4.5. Reversal-атаки 18
4.5.1. Технические сведения по reversal-атакам 18
4.5.2. Общие меры по противодействию reversal-атакам 19
5. Блокировка доменов 19
6. Заключение 20

1. Термины и определения

DDoS (Distributed Denial of Service)	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
FinCERT	Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России
АРМ КБР	Автоматизированное рабочее место клиента Банка России
ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
ОС	Операционная система
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
Ботнет	Компьютерная сеть, состоящая из узлов с запущенным однотипным централизовано управляемым вредоносным ПО
Ботнет-клиент	Зараженное устройство, которым может удаленно управлять злоумышленник
Индикатор компрометации	Данные, позволяющие определить, скомпрометирована ли исследуемая система
Командный сервер	Сервер, как правило в информационно-телекоммуникационной сети Интернет, с которого ведется управление зараженными устройствами
Плагин	Независимо компилируемый программный модуль, динамически подключаемый к основной программе и предназначенный для расширения и(или) использования ее возможностей
Фишинг (Phishing)	Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным, путем маскировки электронного письма или сайта под доверенный аналог
Хост	Устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера
Целенаправленная атака	Компьютерная атака, ориентированная на использование конкретных, известных злоумышленникам уязвимостей в информационной инфраструктуре организаций
Эксплойт (Exploit)	Программное обеспечение или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки

2. Введение

Основная цель функционирования FinCERT – создание центра компетенции в рамках информационного взаимодействия Банка России, организаций ему поднадзорных, компаний-интеграторов, разработчиков ПО, в том числе средств антивирусной защиты, провайдеров и операторов связи, а также для 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.

Для достижения указанных целей выполняются следующие задачи:

- Организация и координация обмена информацией между FinCERT, организациями, поднадзорными Банку России, и правоохранительными органами (Министерство внутренних дел Российской Федерации, Федеральная служба безопасности Российской Федерации, включая информационный обмен с ГосСОПКА);
- Анализ данных о фактах компьютерных атак на организации, поднадзорные Банку России, и подготовка аналитических материалов;
- Подготовка рекомендаций в области обеспечения защиты информации при осуществлении переводов денежных средств.

Настоящий отчет о деятельности FinCERT охватывает период времени за 2-е полугодие 2015 г. и 1-е полугодие 2016 г. и предназначен для широкого круга заинтересованных лиц. Отчет выполнен в двух вариантах:

- Первый содержит описание деятельности FinCERT, а также статистические данные по информационному обмену и основным выявленным атакам (предназначен для размещения на официальном сайте Банка России);
- Второй дополнительно содержит анализ вредоносного программного обеспечения, с помощью которого осуществлялась одна из целенаправленных атак, выявленная за отчетный период, а также индикаторы компрометации этой атаки (предназначен для рассылки участникам информационного обмена).

3. Основные показатели деятельности FinCERT

На сегодняшний день в информационном обмене участвуют **275** кредитных организаций и филиалов. На *рисунке 1* приведено общее количество кредитных организаций, поднадзорных Банку России, присоединившихся к информационному обмену по месяцам.

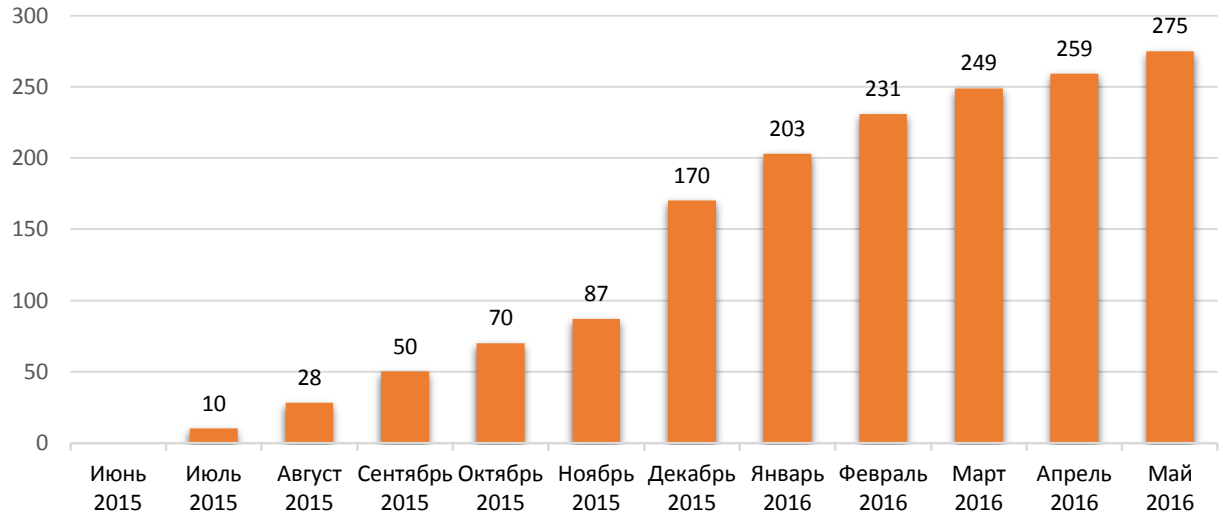

Рисунок 1 – Количество кредитных организаций, присоединившихся к информационному обмену с FinCERT

Также FinCERT осуществляет информационный обмен с правоохранительными органами. Работники FinCERT, в случае необходимости, привлекаются правоохранительными органами в качестве экспертов.

Общее количество участников информационного обмена в разрезе их сферы деятельности приведено на *рисунке 2*.

Рисунок 2 – Общее число участников информационного обмена по типу организации

Основная часть информации об атаках предоставляется участниками информационного обмена. Распределение источников получения информации приведено на *рисунке 3*.

Рисунок 3 – Распределение источников получения информации

При получении от участника информационного обмена сообщения об угрозе, FinCERT проводит ее анализ, по результатам которого выполняется рассылка информационного бюллетеня. Статистика по количеству разосланных бюллетеней приведена на *рисунке 4*.

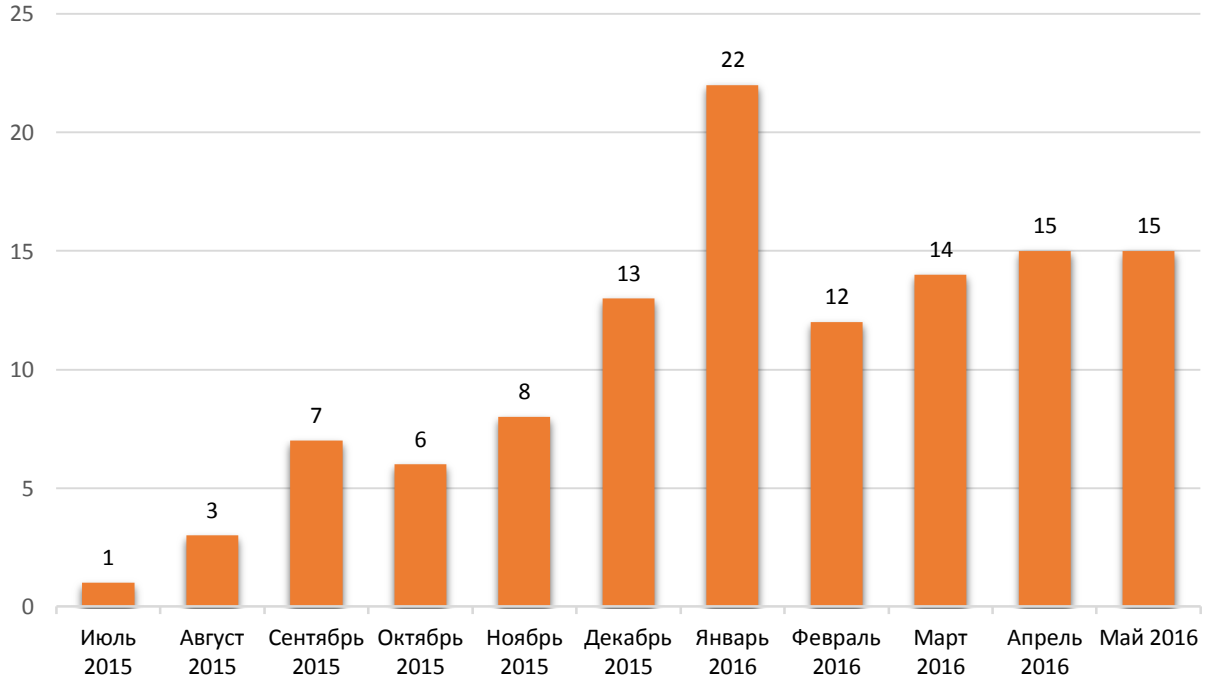

Рисунок 4 – Количество бюллетеней, рассылаемых FinCERT, по месяцам

Процесс обработки FinCERT поступающей информации представлен на *рисунке 5*.

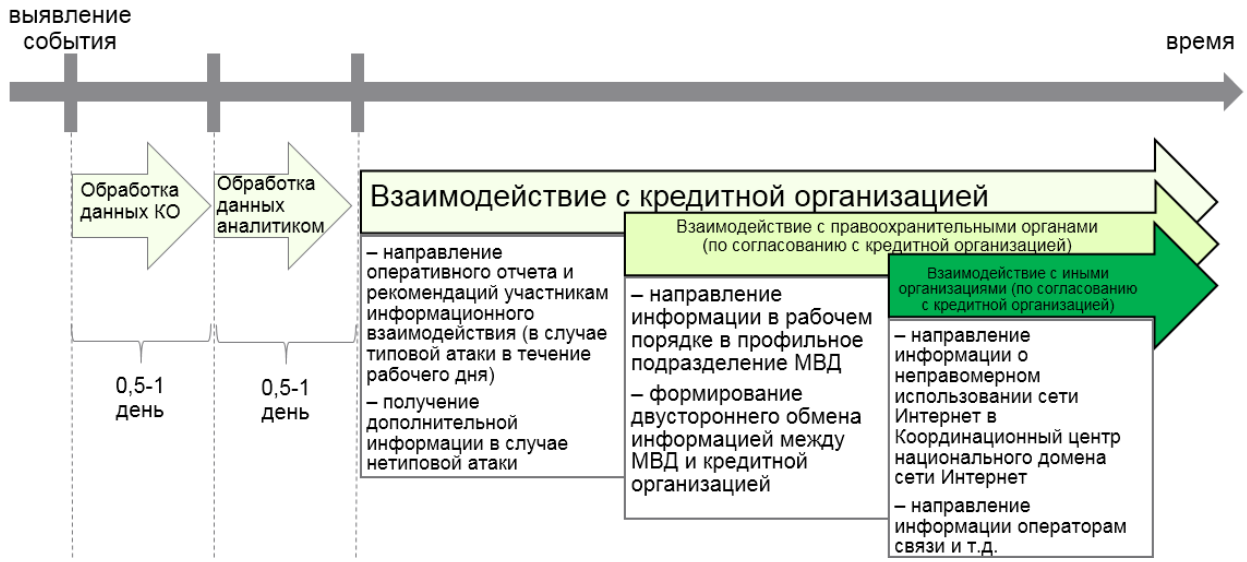

Рисунок 5 – Процесс обработки информации в FinCERT

Информация о способах связи с FinCERT, взаимодействии с FinCERT, требованиях к участникам информационного обмена, а также сведения о целях и задачах FinCERT доступны по адресу http://www.cbr.ru/credit/Gubzi_docs/main.asp?Prtid=fincert.

4. Основные типы атак, зафиксированные FinCERT

За отчетный период были зафиксированы следующие основные типы атак:

- Целенаправленные атаки, связанные с подменой входных данных для АРМ КБР;
- Рассылки электронных сообщений, содержащих вредоносное ПО;
- Атаки, направленные на устройства самообслуживания;
- DDoS-атаки;
- Reversal-атаки.

Каждому из описанных типов атак посвящен отдельный раздел.

4.1. Целенаправленные атаки, связанные с подменой входных данных для АРМ КБР

За отчетный период FinCERT зафиксировал значительное число атак, связанных с подменой входных данных для АРМ КБР (изменение содержимого XML-документа, используемого для формирования электронного сообщения, направляемого в Банк России).

Атака производилась по следующей схеме:

1. В большинстве случаев в кредитную организацию злоумышленниками направлялось электронное письмо, содержащее вредоносное ПО, не детектируемое антивирусными средствами.
2. После заражения вредоносное ПО с помощью SMB-запросов осуществляло сканирование доступного зараженной машине сегмента локальной вычислительной сети, с целью заражения новых рабочих станций.
3. На зараженные машины загружалось дополнительное вредоносное ПО, выполняющее функции ботнет-клиента и обладающее возможностями удаленного

управления (скрытый рабочий стол, в результате чего удаленное управление осуществлялось незаметно для пользователя), а также вредоносное ПО для хищения паролей.

4. Злоумышленники, получив полный контроль над захваченным сегментом локальной вычислительной сети организации, проводили его мониторинг с целью определения АРМ КБР и компьютера, используемого для подготовки XML-документа.

5. Далее осуществлялось создание подложного XML-документа, используемого для формирования электронного сообщения, направляемого в Банк России.

4.1.1. Статистика по атакам, связанным с подменой входных данных для АРМ КБР

За период с октября 2015 г. по март 2016 г. FinCERT зафиксировал **21** атаку на инфраструктуру кредитных организаций. Злоумышленниками были совершены попытки хищения денежных средств на общую сумму порядка **2,87 млрд. руб.** При этом предотвращено хищение порядка **1,6 млрд. руб**., из которых:

- Кредитными организациями, в которых злоумышленники открывали счета с целью осуществления несанкционированных переводов, временно заблокировано порядка **1,1 млрд. руб.**;
- Банком России, в том числе при участии FinCERT, остановлены переводы денежных средств с корреспондентских счетов кредитных организаций на общую сумму порядка **0,57 млрд руб**.

По фактам хищений правоохранительными органами возбуждено **12** уголовных дел.

Основные причины, по которым хищения носили успешный характер:

- Отсутствовало сегментирование локальных вычислительных сетей (в частности, АРМ КБР и компьютер, используемый для подготовки XML-документа, находились в пользовательской локальной вычислительной сети);
- Низкая осведомленность работников кредитных организаций в области информационной безопасности;
- В ряде случаев отсутствовала блокировка автоматического запуска макросов в документах Microsoft Office;
- Пользователям были избыточно присвоены права локального администратора;
- В ряде случаев на атакованных рабочих станциях отсутствовали средства антивирусной защиты, либо их базы были устаревшими;
- Человеческий фактор – ненадлежащий контроль ответственными работниками кредитной организации установленной технологии подготовки, обработки и передачи электронных сообщений, содержащих распоряжение клиентов.

4.1.2. Технические сведения по атакам, связанным с подменой входных данных для АРМ КБР

В январе 2016 г. на форумах в информационно-телекоммуникационной сети Интернет появился исходный код вредоносного ПО, с помощью которого осуществлялась атака, связанная с подменой входных данных для АРМ КБР. FinCERT проанализировал

указанный исходный код. Данные проведенного анализа и индикаторы компрометации по атаке направлены участникам информационного обмена.

4.1.3. Общие меры по противодействию атакам, связанным с подменой входных данных для АРМ КБР

Основная информация по организации мер защиты АРМ КБР представлена в приложении 1 к Договору об обмене электронными сообщениями при переводе денежных средств в рамках платежной системы Банка России, а также в технической документации к АРМ КБР и СКЗИ СКАД «Сигнатура».

В качестве дополнительных мер защиты целесообразно выполнять следующие мероприятия:

1. Сегментирование локальной вычислительной сети (выделение платежного сегмента в отдельный сегмент с минимальными правами доступа и постоянным контролем их изменения);
2. Наличие холодного резерва (вид резервирования, при котором резервные элементы не несут нагрузки (отключены)) компьютера, на котором осуществляется подготовка XML-документа, используемого для формирования электронного сообщения, направляемого в Банк России, и АРМ КБР. Следует отметить, что при заражении самораспространяющимся вредоносным ПО, используемым для осуществления атаки, связанной с подменой входных данных для АРМ КБР, выполнение настоящего мероприятия является временной мерой.
3. Проверка наличия исходящего трафика на серверы центра управления ботнетом в соответствии с данными об адресах, содержащихся в рассылках FinCERT. Подобная проверка может осуществляться с применением:
   - Систем обнаружения/предотвращения вторжений (адреса таких серверов помечаются как подозрительные);
   - Граничного маршрутизатора (при этом необходимо иметь список IP-адресов, обращение к которым разрешено - белый список);
   - Межсетевого экрана, находящегося в демилитаризованной зоне, отслеживающего нетипичный трафик (например, соединения по нетипичным портам).
4. Проверка журналов сервера контроллера домена на наличие подозрительных/аномальных изменений (добавление или удаление пользователей, изменение прав (повышение привилегий) и т.д.).

Контроль выполнения мероприятий 3 и 4 можно автоматизировать с помощью соответствующих правил системы управления событиями информационной безопасности (SIEM) с генерацией уведомления ответственным лицам при срабатывании правила.

4.2. Рассылки электронных сообщений, содержащих вредоносное ПО

Данный тип атак является наиболее распространенным. Сообщения электронной почты, содержащие вредоносное ПО, обладают следующими общими чертами.

Отправители:

- Органы исполнительной власти;
- Крупные телекоммуникационные операторы;

- Профильные интернет-форумы;
- Кредитно-финансовые организации;
- Организации-партнеры;
- Организации-клиенты.

Содержание:

- Требование, поступившее от органов исполнительной власти;
- Рассылка изменений в нормативных актах;
- Взыскание/погашение задолженности/штрафа, оплата услуг;
- Поиск документов для проверки.

Вложения (может быть представлено в виде гиперссылки, при переходе по которой скачиваются перечисляемые вложения):

- Исполняемый файл, замаскированный под документ;
- Архив, содержащий в себе исполняемый файл;
- Специально сформированный файл;
- Файл, содержащий макровирусы.

Общая схема атаки представлена на *рисунке 6*.

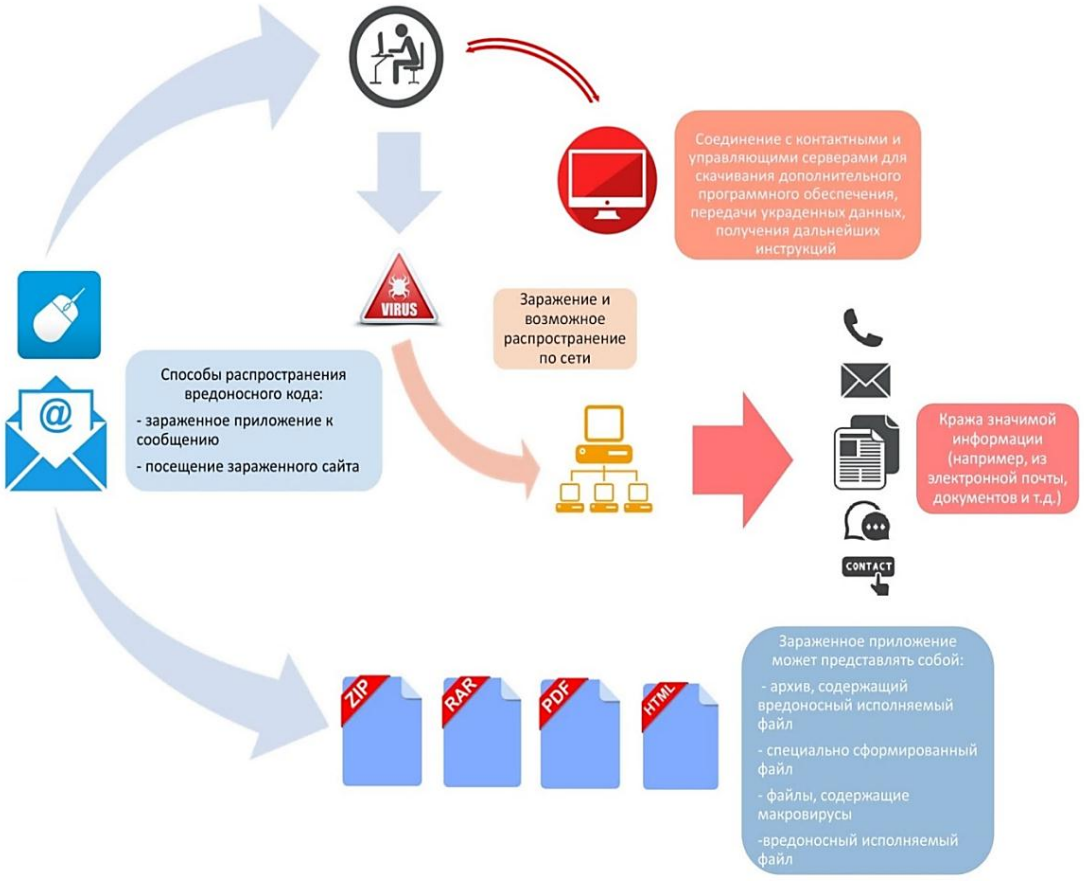

Рисунок 6 – Общая схема атаки с применением вредоносного ПО

FinCERT зафиксировал, в том числе, следующие методы социальной инженерии, использованные злоумышленниками при отправке электронных сообщений, содержащих вредоносное ПО:

- Рассылка фишинговых писем от имени Банка России (так называемые «вакансии», отличительной чертой которых являлось наличие вложение с заголовком вида «вакансия_№XX.doc), во вложении содержался макрос, выполняющий скачивание загрузчика вредоносного ПО. Многие пользователи открывали письма исключительно из любопытства, при этом осознанно включая макросы в Microsoft Word, которые «по умолчанию» обычно заблокированы. Рассылки были не персонифицированы.
- Рассылка фишинговых писем от имени клуба «Антидроп» (некоммерческое объединение специалистов по информационной безопасности в финансовой сфере). Рассылки были персонифицированы.
- Рассылка «FakeCERT», при которой под видом бюллетеня FinCERT с домена fincert.net были разосланы фишинговые письма, содержащие тот же загрузчик. Следует отметить, что большинство участников информационного обмена письмо не открыли, сообщив о рассылке в FinCERT.

4.2.1. Статистика по рассылкам электронных сообщений, содержащих вредоносное ПО

В рамках текущей деятельности FinCERT проводит экспертизу направляемых участниками информационного обмена экземпляров вредоносного ПО. В большинстве случаев на момент получения экземпляра вредоносного ПО он не детектируется средствами антивирусной защиты. Основной целью проводимой экспертизы является выявление индикаторов компрометации.

По результатам проведенной экспертизы вредоносного ПО FinCERT, исходя из следующих критериев, подготавливает и рассылает бюллетень:

- В случае массовости обращений участников информационного обмена в отношении экземпляра вредоносного ПО и/или его модификаций. На сегодняшний день рассылка вредоносного ПО считается массовой при ее выявлении у **15** и более участников информационного обмена;
- Вредоносное ПО используется для осуществления целенаправленной атаки;
- Выявление нового образца вредоносного ПО, функционирующего на мобильных устройствах и направленного на хищение денежных средств у клиентов кредитных организаций.

Статистика по типам вредоносного ПО, по которым FinCERT производил рассылки бюллетеней, приведена на *рисунке 7*.

За отчетный период FinCERT выполнил **96** рассылок подобных бюллетеней.

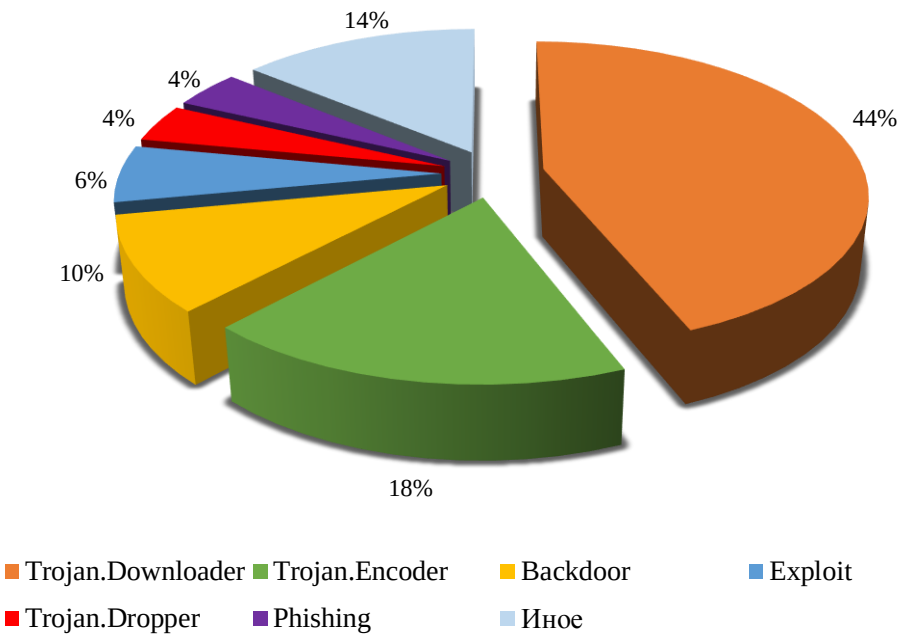

Рисунок 7 – Статистика по типам вредоносного ПО

Наиболее массовая доля рассылок вредоносного ПО приходится на вредоносное ПО типа Trojan.Downloader. В преобладающем количестве случаев (более **80%**) данный тип вредоносного ПО применялся для загрузки вирусов-шифровальщиков.

4.2.2. Технические сведения по рассылкам электронных сообщений, содержащих вредоносное ПО

Trojan.Downloader представляет собой вредоносное ПО, предназначенное для скрытой загрузки и установки на компьютер различного вредоносного ПО и троянских программ.

Подобного рода ПО содержит в себе заранее прописанные имена и расположение файлов, скачиваемых загрузчиком с управляющего сервера. Зачастую загруженное подобным образом вредоносное ПО прописывается троянской программой в автозагрузке.

Trojan.Encoder представляет собой вредоносное ПО, шифрующее файлы на жестком диске компьютера и требующее деньги за их расшифровку. В результате действия указанного вредоносного ПО зашифрованными могут оказаться, среди прочего, файлы *.doc, *.docx, *.pdf, *.jpg, *.rar.

За отчетный период FinCERT зафиксировал несколько крупных кампаний рассылок троянских программ-шифровальщиков от имени государственных компаний, различных кредитно-финансовых учреждений и иных организаций.

Отличительной особенностью некоторых рассылок является изменение вредоносного вложения с каждой итерацией рассылки.

Backdoor представляет собой вредоносное ПО, назначением которого является скрытое от пользователя удаленное управление злоумышленником компьютером жертвы. Часто подобного типа программы используются для создания ботнетов.

Trojan.Dropper представляет собой вредоносное ПО, предназначенное для скрытной установки на компьютер пользователя ПО, содержащегося в теле троянской программы. В

некоторых случаях пользователю приходят ложные сообщения об ошибке в ПО, при открытии файла, ошибке в архиве и т.д. Обычно вредоносное ПО сохраняется троянской программой в каталоги Windows, в том числе в системные или временные каталоги.

4.2.3. Общие меры по противодействию

Меры по противодействию подобного типа атакам, среди прочего, могут включать в себя:

1. Организационные меры: проведение обучения работников организации по вопросам обеспечения информационной безопасности (как минимум, рекомендации не открывать вложения в письмах, пришедших из недоверенных источников, и письма, содержание которых не относится к сфере деятельности работника), постоянный контроль знаний работников (например, выборочные проверки в виде отправки службой информационной безопасности фишингового электронного письма), а также проведение иных мероприятий, направленных на повышение грамотности работников в области информационной безопасности.
2. Технические меры на компьютерах работников: установка запрета на использование учетных записей с расширенными правами доступа, если это не входит в круг должностных обязанностей работника; установка запрета для работника на управление средствами антивирусной защиты; контроль и обязательная проверка подключаемых носителей информации средствами антивирусной защиты, а также своевременное обновление антивирусных баз и сигнатур хостовых систем обнаружения вторжений.
3. Технические меры на почтовых серверах: использование проверки SPF записи (при наличии технической возможности), использование почтовых средств антивирусной защиты, использование спам-листов. При подозрении на вложение, содержащее вредоносное ПО, целесообразно изъятие указанного вложения из электронного письма и перемещение его в «карантин». При этом, доставляя электронное письмо до конечного пользователя, необходимо информировать его об изъятии подозрительного вложения. В случае необходимости восстановления (разблокировки) вложения рекомендовать обращаться в подразделение, отвечающее за обеспечение информационной безопасности в организации.

4.3. Атаки, направленные на устройства самообслуживания

За отчетный период FinCERT зафиксировал рост интереса злоумышленников к устройствам самообслуживания, в том числе банкоматам и POS-терминалам.

4.3.1. Статистика по атакам, направленным на банкоматы

На сегодняшний день зафиксировано **17** случаев, связанных с несанкционированным доступом к ПО банкомата и последующей попыткой хищения денежных средств. При реализации атак, направленных на банкоматы, злоумышленниками были совершены покушения на хищение денежных средств на общую сумму свыше **100 млн. руб**.

4.3.2. Технические сведения по атакам, направленным на банкоматы

За отчетный период зафиксировано 3 типа атак:

1. Атака, направленная на подмену хоста. В большинстве случаев, конечная цель подобной атаки – вызвать т.н. «джекпоттинг», т.е. перевести устройство в такое состояние, при котором оно выдает все имеющиеся денежные средства атакующему. Суть атаки состоит в следующем: злоумышленник получает доступ к USB-портам банкомата (через использование универсального ключа для открытия, либо непосредственное физическое воздействие), используя съемный носитель информации, устанавливает вредоносное ПО, после чего банкомат переходит в режим супервизора, но при этом с точки зрения легитимного хоста – устройство находится в режиме клиентского обслуживания. По факту же, оно ожидает команды с пин-пада или от вредоносного ПО, либо работает в автоматизированном режиме;
2. Атака, направленная на получение контроля над банкоматом. В данном случае, в банкомат ставится дополнительное устройство (как правило, на базе Android, но есть варианты, реализованные на Arduino / Raspberry), после чего банкомат переводится в обычный режим работы, при этом злоумышленник имеет возможность удаленного доступа к банкомату.
3. «Прямой диспенс». Суть атаки заключается в подключении к диспенсеру (либо через отключение диспенсера от общей шины банкомата, либо через подмену ПО банкомата) с дальнейшей отправкой команды на опустошение кассет. Злоумышленниками используется пароль «по умолчанию» для входа в BIOS банкомата, после чего может быть изменен порядок загрузки и подключено внешнее устройство, с которого осуществляется загрузка с последующим получением доступа к сервисному режиму работы банкомата и контролем над диспенсером. Указанные действия позволяют злоумышленнику выполнить команду (AFD) на опустошение диспенсера.

4.3.3. Общие меры по противодействию атакам, направленным на банкоматы

Основные рекомендации по противодействию подобного типа атакам приведены в таблице 1.

Таблица 1 – Основные меры противодействия атакам, направленным на банкоматы

№	Мера противодействия	Разъяснение
1	Смена пароля BIOS	Смена пароля для входа в BIOS с предустановленного производителем
2	Уточнить возможность установки двухфакторной аутентификации для входа в BIOS.	Свяжитесь с производителем банкомата для выяснения подобной возможности, при необходимости обновите BIOS
3	Установка сигнализации на открытие верхнего кабинета банкомата, использование уникальных ключей для сервис-блоков, установка дополнительных замков, затрудняющих вскрытие банкомата	-

Таблица 1 – Основные меры противодействия атакам, направленным на банкоматы

№	Мера противодействия	Разъяснение
5	Активировать технологию Intel AMT	Активация технологии позволит управлять изменениями паролей BIOS, контролировать вход в BIOS
6	Обновить ПО банкомата	Следует отслеживать, чтобы ПО банкомата было в актуальном состоянии
7	Установка защищенного протокола обмена	Проверить, что используются протоколы SPEAR / FMPP для обмена командами с диспенсером, установить максимальный уровень безопасности
9	Обновить BIOS	Обновить BIOS до версии, в которой поддерживается двухфакторная аутентификация, после чего активировать ее
10	Убедиться (по возможности), что используются последние версии протоколов	Убедиться, что используется протокол версии SPEAR II при использовании SPEAR
11	Установка специализированного ПО для мониторинга состояния банкомата, в т.ч. и для отслеживания вскрытия верхнего кабинета и(или) несанкционированного отключения питания, ПО контроля целостности	-

4.3.4. Статистика по атакам, направленным на POS-терминалы

В конце 2015 г. FinCERT зафиксировал рост интереса злоумышленников к POS-терминалам, в частности, отмечено появление предложений о продаже доработанных POS-терминалов, обладающих дополнительным функционалом, таким как сохранение дампа карты с PIN-кодом, возможностью удаленной загрузки сохраненных на POS-терминале данных. Основная география распространения – США, известны случаи выявления в Европе.

Сохраняется тенденция работы злоумышленников совместно с работниками предприятий сферы обслуживания, которые имеют практически бесконтрольный доступ к POS-терминалу и в части случаев – к платежной карте клиента.

4.3.5. Технические сведения по атакам, направленным на POS-терминалы

FinCERT отмечает появление вредоносного ПО, предназначенного для заражения кассового терминала, работающего под управлением ОС Windows (в т.ч. Embedded-версии), с возможностью написания для него плагинов.

Вредоносное ПО обладает, как минимум, возможностями перехвата данных, вводимых с клавиатуры (кейлоггер), дистанционного управления и получения данных из оперативной памяти POS-терминала. Основные модули (за исключением загрузчика ПО) не детектируются средствами антивирусной защиты. К модулю, обеспечивающему

контроль POS-терминала, могут быть подключены различные плагины, обеспечивающие дополнительный функционал. Одно из названий данного вредоносного ПО – ModPOS.

Помимо вышеуказанного ModPOS набирает популярность вредоносное ПО вида FastPOS. Основной особенностью данного вида вредоносного ПО является незамедлительная отправка похищенных данных на командный сервер, т.е. отсутствует хранение указанных данных в памяти устройства.

4.3.6. Общие меры по противодействию атакам, направленным на POS-терминалы

Основные меры противодействия атакам, направленным на POS-терминалы, приведены в *таблице 2.*

Таблица 2 – Основные меры противодействия атакам, направленным на POS-терминалы

№	Мера противодействия	Разъяснение
1	Проверка исходящего трафика на соединение с командными сервером	Рекомендуется внести соответствующие сигнатуры для систем IDS/IPS, содержащие адреса командных серверов
2	Контроль за внедрениями в системные процессы (может обеспечиваться антивирусным ПО)	При заражении происходит внедрение кода вредоносного ПО в системные процессы
3	Контроль за созданием подозрительных файлов	Рекомендуется контролировать создание файлов, и при необходимости, принимать меры к их удалению. Ввиду факта возможного затруднения в обнаружении подозрительных файлов – рекомендуется обращать внимание на записи в логах о соединениях с командными серверами и осуществлять поиск файлов, которые были созданы после первого соединения с командным сервером
4	Контроль актуальности антивирусных баз	Рекомендуется контролировать актуальность антивирусных баз на хостах, подключенных к POS-устройствам

Сведения по индикаторам компрометации атаки (с использованием вредоносного ПО ModPOS), направленной на POS-терминалы, доведены до участников информационного взаимодействия.

4.4. DDoS-атаки

Целью DDoS-атак является отказ в обслуживании легитимных клиентов, вплоть до полной невозможности работы с сервисом. Причинами атаки могут быть: недобросовестная конкуренция, хактивизм (действия, когда атакующий в большей степени мотивирован идеологическими мотивами), политические мотивы и иные причины.

В некоторых случаях, DDoS-атака используется для сокрытия факта целенаправленной атаки.

4.4.1. Статистика по DDoS-атакам

Наиболее масштабной DDoS-атакой за отчетный период является атака группировки Armada Collective, участники которой перед началом атаки присылали письмо-требование выкупа для предотвращения / прекращения DDoS-атаки.

Следует отметить низкую активность участников информационного обмена, не уведомляющих в силу различных причин FinCERT о факте проведения DDoS. В настоящее время FinCERT формирует базу внешних (периметровых) IP-адресов участников информационного обмена. Цель указанного мероприятия – получение, в том числе и от ГосСОПКА, информации об атаках и подозрительной активности в направлении каждого участника информационного обмена.

Распределение DDoS-атак приведено на *рисунке 8*.

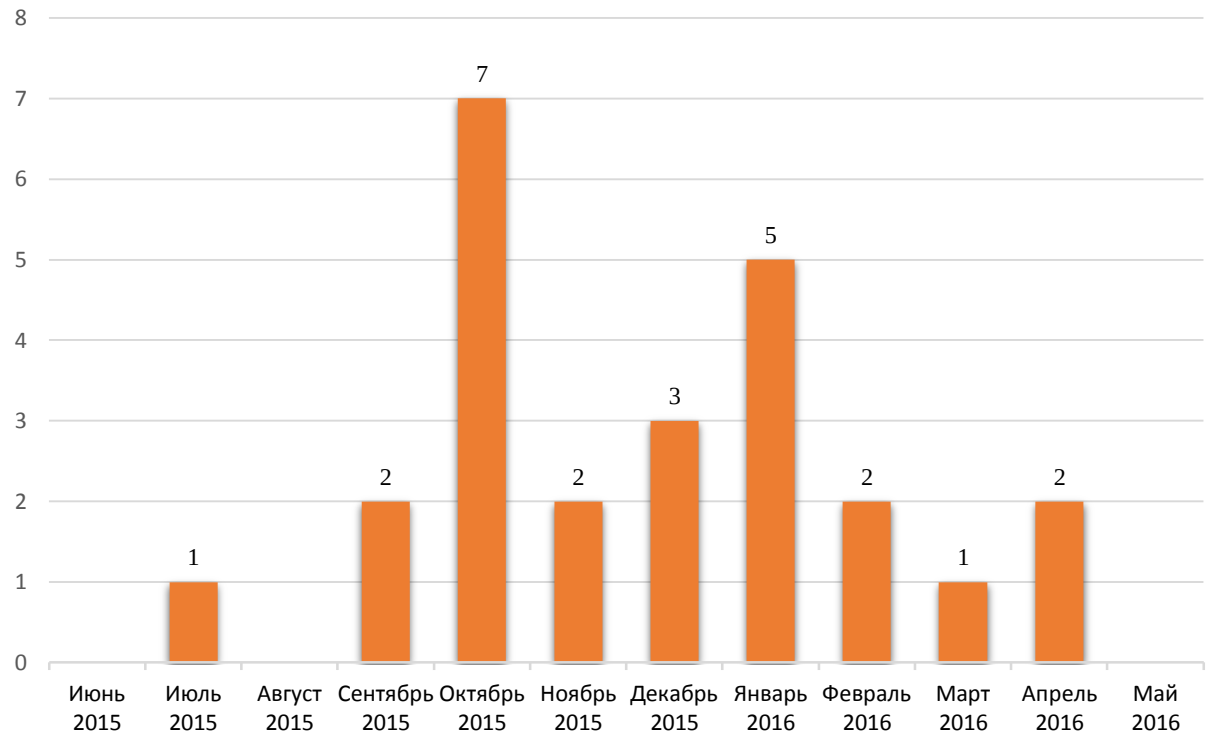

Рисунок 8 – Статистика обращений в FinCERT, связанных с DDoS-атаками

Мировая практика[1] свидетельствует о тенденции к увеличению DDoS-атак как инструмента вымогательства, остальные мотивации, такие как хактивизм, месть и спортивный интерес остаются практически неизменными.

4.4.2. Технические сведения по DDoS-атакам

Как правило, большинство атак являются мультивекторными: для усложнения атаки используется одновременно несколько способов воздействия на целевую систему, тем самым, защититься от нее становится значительно труднее. Изменение вектора не требует существенных временных затрат.

[1] Данные подготовлены совместно с Radware (www.radware.com) в рамках информационного взаимодействия и сотрудничества

Распределение атак по типам и частоте возникновения за отчетный приведено на *рисунке 9*.

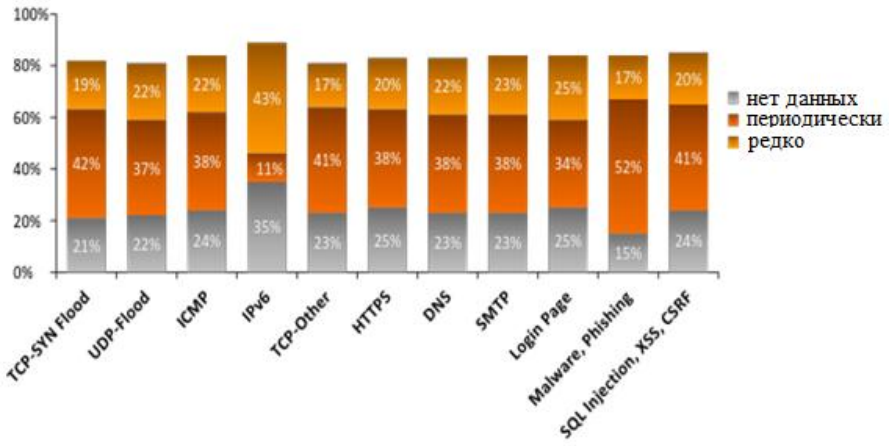

Рисунок 9 – Распределение атак по типу и частоте возникновения

4.4.3. Общие меры по противодействию DDoS-атакам

Для минимизации риска реализации подобного типа атак рекомендуется выполнять следующие мероприятия:

- Определение показателей использования сети (типы трафика и его объём), характерных для организации. Отклонение показателей от характерных значений может свидетельствовать о начале атаки.
- Формирование «дорожной карты» действий работников организации в случае выявления DDoS-атаки.
- Апробация разработанной «дорожной карты» действий работников организации в случае выявления DDoS-атаки и ее доработка по результатам апробации.
- Использование принципа «запрещено все, что не разрешено явно» при настройке сетевого оборудования.

4.5. Reversal-атаки

За отчетный период FinCERT зафиксировал атаку с использованием подложных сообщений об отмене платежной операции (reversal).

Атака связана с особенностью обработки сообщений об отмене авторизации переводов денежных средств процессинговым центром. В большинстве случаев, процессинговые центры не проверяют подлинность подобного запроса, в связи с отсутствием контроля ряда полей указанной операции.

4.5.1. Технические сведения по reversal-атакам

Схематически reversal-атака показана на *рисунке 10*.

Рисунок 10 – Схема reversal-атаки

4.5.2. Общие меры по противодействию reversal-атакам

Для минимизации риска реализации подобного типа атак рекомендуется выполнять следующие мероприятия:

- Контроль доступа и предоставления прав доступа к системам, с использованием которых осуществляется передача платежных сообщений;
- Контроль соблюдения порядка формирования, удостоверения, передачи операционному центру платежной системы электронных сообщений;
- Контроль доступа работников к проведению операций reversal;
- Сверка реквизитов операции отмены и исходной операции, в частности, следующих полей электронных сообщений: идентификатор эквайрера, идентификатор транзакции, Retrieval Reference Number (RRN), AIR – код авторизации;
- Контроль нетипичных операций reversal, а также аномальных изменений расходного лимита;
- Мониторинг нештатного функционирования объектов инфраструктуры;
- Своевременная установка обновлений ПО процессинговых центров.

5. Блокировка доменов

FinCERT имеет возможность уведомлять регистраторов доменов о доменах, с которых осуществляется рассылка вредоносного ПО, а также осуществляется сбор данных для осуществления несанкционированных переводов денежных средств с использованием различных электронных средств платежа. Основные критерии, по которым в отношении домена могут быть подготовлены предложения о блокировке:

- С домена осуществляется рассылка вредоносного ПО (срабатывание средств антивирусной защиты, анализ FinCERT, подтверждение от компетентной организации[2]);
- На домене находится сайт, собирающий данные платежных карт (ФИО, номер, срок действия, код проверки подлинности карты);
- На домене находится сайт, имитирующий ресурсы Банка России;
- Домен является командным сервером ботнета (согласно данным Threat Intelligence; информации, полученной от участников информационного обмена, правоохранительных органов; данным, собранным FinCERT);
- На домене содержатся материалы фишингового содержания (в отношении организаций, поднадзорных Банку России).

В рамках указанной деятельности FinCERT взаимодействует с:

- Координационным центром национального домена сети Интернет (зоны .RU, .РФ, .SU);
- Международными ассоциациями (зоны .COM, .NET).

Начиная с 31 марта по 24 мая 2016 г. FinCERT направил информацию о **118** доменах различной мошеннической тематики, подлежащих блокировке (все **118** доменов по итогам рассмотрения направленной информации заблокированы регистраторами).

6. Заключение

На сегодняшний день в информационном обмене с FinCERT участвуют **275** кредитных организаций и филиалов, **9** небанковских кредитных организаций, **6** иностранных кредитных организаций, **6** разработчиков ПО, **6** органов государственной власти, **5** платежных систем, **3** оператора связи и **7** иных организаций.

Кроме того FinCERT осуществляет информационный обмен с правоохранительными органами (Министерство внутренних дел Российской Федерации, Федеральная служба безопасности Российской Федерации, включая информационный обмен с ГосСОПКА). Работники FinCERT, в случае необходимости, привлекаются правоохранительными органами в качестве экспертов.

В рамках деятельности FinCERT за отчетный период были зафиксированы следующие основные типы атак, основная часть данных о которых была предоставлена участниками обмена:

- Целенаправленные атаки, связанные с подменой входных данных для АРМ КБР. Зафиксирована **21** атака на инфраструктуру кредитных организаций, в результате которых злоумышленниками были совершены покушения на хищение денежных средств на общую сумму порядка **2,87 млрд. руб.** При этом предотвращено хищение порядка **1,6 млрд. руб.**
- Рассылки электронных сообщений, содержащих вредоносное ПО. В рамках текущей деятельности FinCERT проводит экспертизу направляемых участниками информационного обмена экземпляров вредоносного ПО. Основной целью проводимой экспертизы является выявление индикаторов компрометации. По результатам проведенной экспертизы вредоносного ПО FinCERT, исходя из критериев массовости рассылки электронных сообщений, содержащих вредоносное ПО, а также уровня его опасности,

[2] Компетентной организацией считается организация, имеющая аккредитацию в Координационном центре национального домена сети Интернет (https://cctld.ru/ru/activities/competent/)

подготавливает и рассылает бюллетень. FinCERT выполнил **96** рассылок подобных бюллетеней.

- Атаки, направленные на устройства самообслуживания (банкоматы и POS-терминалы). Выявлено 17 атак на банкоматы, отличительной особенностью которых являются: несанкционированный доступ злоумышленника к ПО банкомата и последующая попытка хищения денежных средств. При реализации атак, направленных на банкоматы, злоумышленниками были совершены попытки хищения денежных средств на общую сумму свыше 100 млн. руб. В конце 2015 г. FinCERT зафиксировал рост интереса злоумышленников к POS-терминалам, в частности, отмечено появление предложений о продаже доработанных POS-терминалов, обладающих дополнительным функционалом, таким как сохранение дампа карты с PIN-кодом, возможностью удаленной загрузки сохраненных на POS-терминале данных. Основная география распространения – США, известны случаи выявления в Европе.
- DDoS-атаки. FinCERT зафиксировал **25** DDoS-атак. Наиболее масштабной DDoS-атакой за отчетный период является атака группировки Armada Collective, участники которой перед началом атаки присылали письмо-требование выкупа для предотвращения / прекращения DDoS-атаки.
- Reversal-атаки. Зафиксированная FinCERT атака связана с особенностью обработки сообщений об отмене авторизации перевода денежных средств процессинговым центром, вследствие отсутствия достаточных контролей ряда полей указанной операции. В большинстве случаев, процессинговые центры не проверяют подлинность подобного запроса.

FinCERT имеет возможность уведомлять регистраторов доменов о доменах, с которых осуществляется рассылка вредоносного ПО, а также осуществляется сбор данных для выполнения несанкционированных переводов денежных средств с использованием различных электронных средств платежа.

В рамках указанной деятельности FinCERT взаимодействует с:

- Координационным центром национального домена сети Интернет (зоны .RU, .РФ, .SU);
- Международными ассоциациями (зоны .COM, .NET).

Начиная с 31 марта по 24 мая 2016 г. FinCERT направил информацию о **118** доменах различной мошеннической тематики, подлежащих блокировке (все **118** доменов по итогам рассмотрения направленной информации заблокированы регистраторами).