ОТЧЕТ ЦЕНТРА МОНИТОРИНГА И РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ АТАКИ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ ДЕПАРТАМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА РОССИИ
1.09.2017 – 31.08.2018

БАНК РОССИИ
ФИНЦЕРТ

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ 2

БЕЗОПАСНАЯ СРЕДА ДЛЯ ФИНАНСОВОГО РЫНКА 3

ВВЕДЕНИЕ 4

1. ОБМЕН ИНФОРМАЦИЕЙ ОБ УГРОЗАХ. УЧАСТНИКИ, ЗАДАЧИ, ИНСТРУМЕНТЫ 6

- УЧАСТНИКИ ИНФОРМАЦИОННОГО ОБМЕНА 6
- ИНФОРМИРОВАНИЕ УЧАСТНИКОВ ОБМЕНА 11
- АВТОМАТИЗАЦИЯ ИНФОРМАЦИОННОГО ОБМЕНА 12
- РАБОТА С ОБЩЕСТВЕННОСТЬЮ 14
- ВЫВОДЫ И ПРОГНОЗЫ 18

2. ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ 19

- НУЛЕВЫЕ ПОТЕРИ БАНКОВ И ИХ КЛИЕНТОВ В ХОДЕ ЧМ-2018 19
- ВРЕДОНОСНЫЕ САЙТЫ, СМС-РАССЫЛКИ И КОЛЛ-ЦЕНТРЫ МОШЕННИЧЕСКИХ СТРУКТУР 20
- ТЕХНИЧЕСКИЙ АНАЛИЗ КОМПЬЮТЕРНЫХ АТАК 24
- ЦЕЛЕВЫЕ АТАКИ НА ОРГАНИЗАЦИИ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ 25
- НЕЦЕЛЕВЫЕ (СПАМ-АТАКИ) НА ОРГАНИЗАЦИИ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ 31
- АТАКИ НА УСТРОЙСТВА САМООБСЛУЖИВАНИЯ 33
- МОШЕННИЧЕСТВО С ОТМЕНОЙ ТРАНЗАКЦИЙ (TRF – TRANSACTION REVERSAL FRAUD) 37
- АТАКИ НА КЛИЕНТОВ КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ 38
- АТАКИ НА КЛИЕНТОВ – ФИЗИЧЕСКИХ ЛИЦ 39
- ВЫВОДЫ И ПРОГНОЗЫ 42

Настоящий отчет подготовлен Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России) Департамента информационной безопасности Банка России.

Список сокращений

БПО	Банковское программное обеспечение
ВПО	Вредоносное программное обеспечение
ДБО	Дистанционное банковское обслуживание
Мобильные устройства	Абонентские устройства мобильной связи, мобильные телефоны, смартфоны, коммуникаторы и другие устройства, используемые клиентами кредитных организаций при осуществлении переводов денежных средств
Несанкционированная операция	Несанкционированная операция по переводу денежных средств
ПО	Программное обеспечение
Положение Банка России № 382-П	Положение Банка России от 9.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»
Положение Банка России № 552-П	Положение Банка России от 24.08.2016 № 552-П «О требованиях к защите информации в платежной системе Банка России»
Федеральный закон № 167-ФЗ	Федеральный закон от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств»
Федеральный закон № 187-ФЗ	Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Фишинг	Адресуемая с использованием домена информационная система применяется для получения от третьих лиц (пользователей системы) конфиденциальных сведений за счет введения этих лиц в заблуждение относительно ее принадлежности (подлинности) вследствие сходства доменных имен, оформления или содержания информации
ЭСП	Электронное средство платежа
CNP-транзакция	Транзакция типа «Card Not Present» – операция, осуществленная в сети Интернет с использованием реквизитов платежной карты (без предъявления ее материального носителя)

Примечание: в случае если не указано иное, в обзоре представлена информация о количестве и объеме несанкционированных операций, совершенных с использованием платежных карт, эмитированных кредитными организациями, зарегистрированными на территории Российской Федерации.

Безопасная среда для финансового рынка

Обращение Заместителя Председателя Банка России Д.Г. Скобелкина для Годового отчета ФинЦЕРТ

Уважаемые коллеги!

Прошедший год для ФинЦЕРТ был очень насыщенным. Принят ряд важных для взаимодействия с рынком нормативных актов, создана и работает автоматизированная система взаимодействия с кредитными организациями АСОИ ФинЦЕРТ. Благодаря ранее проделанной работе три волны резонансных атак вирусов прошли для банков с минимальными последствиями. Совместная подготовка ФинЦЕРТ и организаций кредитно-финансовой сферы к чемпионату мира по футболу свели к нулю их потери от действий мошенников.

По итогам анализа поступивших за год сообщений по каналам информационного обмена мы с удовлетворением отмечаем возросшую в несколько раз активность его участников. Данные, поступавшие от банков и других организаций, помогли ФинЦЕРТ инициировать разделегирование более 1,5 тыс. доменов фишинговых ресурсов.

Также мы наблюдаем существенное снижение объема хищений со счетов юридических лиц. Тем не менее часть атак по-прежнему успешна, и основная причина этого – человеческий фактор.

По-прежнему в тренде остаются атаки на устройства самообслуживания. В основном это blackbox, а также атаки вида TRF (Transaction Reversal Fraud – мошенничество с отменой транзакций), а вот число атак вида «скимминг» и «шимминг» неуклонно снижается.

Если говорить о наших планах, то их все можно разделить на три блока. Это автоматизация информационного обмена, усиление международного взаимодействия, а также укрепление и развитие технической базы и команды ФинЦЕРТ.

К середине 2019 г. будет окончательно автоматизирован сбор информации об инцидентах на стороне участника обмена и введена в действие система «Фид-АнтиФрод» – база данных об операциях по переводу денежных средств без согласия клиента.

В области международного сотрудничества приоритетом останется взаимодействие со странами ЕАЭС, финансовым регуляторам которых мы будем помогать создавать системы и центры мониторинга и реагирования на компьютерные атаки, и затем все вместе будем создавать единую доверенную платежную среду. Наряду с этим мы начинаем проработку возможности заключения соглашений об информационном взаимодействии в сфере кибербезопасности со странами БРИКС.

Мы также планируем дооснастить лабораторию технического анализа устройствами для проведения исследований, что в разы повысит их эффективность, а также развивать работу по раннему поиску компетентных сотрудников – в том числе в рамках работы с учебным центром «Сириус».

Заместитель Председателя Банка России *Д.Г. Скобелкин*

Введение

Использование информационных технологий и основанных на них бизнес-решений является одним из основных инструментов снижения издержек финансовых организаций и повышения их конкурентоспособности. Однако наряду с этим возникают и новые виды рисков, отсутствие должного внимания к которым представляет серьезную угрозу для финансовой стабильности, прав и интересов потребителей финансовых услуг.

В 2015 г. Банк России принял решение объединить участников финансового рынка в едином информационном пространстве, где они будут получать оперативные данные об актуальных киберугрозах и набор программных средств и рекомендаций, применение которых минимизирует ущерб и потери этих организаций и их клиентов. Для этого в Банке России был создан Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности (ФинЦЕРТ).

Сегодня участниками информационного обмена и партнерами ФинЦЕРТ являются как организации кредитно-финансовой сферы, так и их контрагенты – системные интеграторы, разработчики антивирусного программного обеспечения. Большой вклад в работу сообщества под эгидой ФинЦЕРТ вносит участие в информационном обмене телеком-провайдеров, операторов связи, иностранных финансовых организаций, регуляторов, групп реагирования на инциденты, правоохранительных и других государственных органов.

До настоящего времени участие в информационном обмене носило добровольный характер, однако с 1 июля 2018 г. кредитные организации[1] должны будут уведомлять Банк России о выявленных инцидентах[2].

За годы работы информационный обмен на базе ФинЦЕРТ продемонстрировал значительные результаты: уменьшение количества и объема несанкционированных операций; снижение киберрисков; рост защищенности прав и интересов клиентов российских банков; повышение уровня финансовой устойчивости участников кредитно-финансовой сферы.

Начиная с 2020 г. оперативное получение информации о киберугрозах станет одним из инструментов снижения киберриска, расходы на покрытие потерь от которого будут влиять на размер капитала кредитных организаций.

Штат ФинЦЕРТ включает 38 квалифицированных специалистов, имеющих богатый практический опыт в области анализа защищенности и уязвимостей информационных систем, а также векторов атак, реализуемых на их основе. Сотрудники ФинЦЕРТ имеют высшее техническое и экономическое образование (у троих – ученая степень), полученное в таких высших учебных заведениях, как МГТУ им. Баумана, НИЯУ МИФИ и МГУ им.

---

[1] *Операторы платежных систем, операторы услуг платежной инфраструктуры и операторы по переводу денежных средств.*

[2] *Положение Банка России № 382-П.*

М.В. Ломоносова. Помимо этого, специалисты ФинЦЕРТ регулярно проходят курсы, направленные на повышение квалификации. У многих есть опыт работы в банковской сфере и правоохранительных органах. Средний возраст сотрудников составляет 34 года.

1. Обмен информацией об угрозах. Участники, задачи, инструменты

УЧАСТНИКИ ИНФОРМАЦИОННОГО ОБМЕНА

Основной задачей ФинЦЕРТ является обеспечение информационной безопасности осуществления финансовых операций, в том числе переводов денежных средств в кредитно-финансовой сфере. Для этого ФинЦЕРТ наделен полномочиями по организации информационного обмена о киберинцидентах с организациями, участвующими в проведении финансовых операций.

Сегодня в информационном обмене ФинЦЕРТ участвуют 718 организаций. За последний год их число увеличилось на 16%. Подавляющее большинство участников обмена составляют банки, еще примерно четверть – это иные финансовые организации, госструктуры, телеком-провайдеры, операторы сотовой связи, а также IT-компании (в том числе в сфере кибербезопасности), энергетические и промышленные предприятия.

Рисунок 1
Участники информационного обмена (%)

ФинЦЕРТ ведет сбор и обработку поступившей от них информации о произошедших и предотвращенных компьютерных атаках, пострадавших организациях и их клиентах, а также о лицах и организациях, причастных к совершению компьютерных атак, средствах и методах их совершения. На основе анализа получаемых данных ФинЦЕРТ уведомляет участников обмена об угрозах в области информационной безопасности с целью снижения объемов хищений денежных средств и, как следствие, поддержания устойчивости финансовых организаций и защиты прав и интересов их клиентов.

Информационный обмен с поднадзорными организациями

Три года назад серьезный всплеск хищений денежных средств со счетов физических и юридических лиц выявил ряд пробелов в сфере безопасности электронных платежей. Оказалось, что у банков нет ни четкого понимания, с чем им нужно бороться, ни юридического инструментария для такой борьбы. Сотрудники некоторых банков договаривались между собой об обмене данными об участниках схем хищений денежных средств («дропперах»), однако фактически такой обмен являлся разглашением конфиденциальной информации и его участникам могли угрожать санкции вплоть до уголовных.

Создание ФинЦЕРТ стало первым шагом к ликвидации этих пробелов. В течение трех лет добровольное участие в информационном обмене позволяло как ФинЦЕРТ, так и банкам наращивать объем информации, позволяющей оперативно выявлять угрозы и своевременно на них реагировать. Как следствие, уже к февралю 2018 г. объем ущерба от несанкционированных переводов по счетам юридических и физических лиц существенно снизился.

Одновременно с повышением качества экспертизы Банк России вел разработку нормативных актов для создания правовых основ определения, приостановки и возврата несанкционированных переводов. В ито-

Рисунок 2
Поднадзорные организации – участники обмена

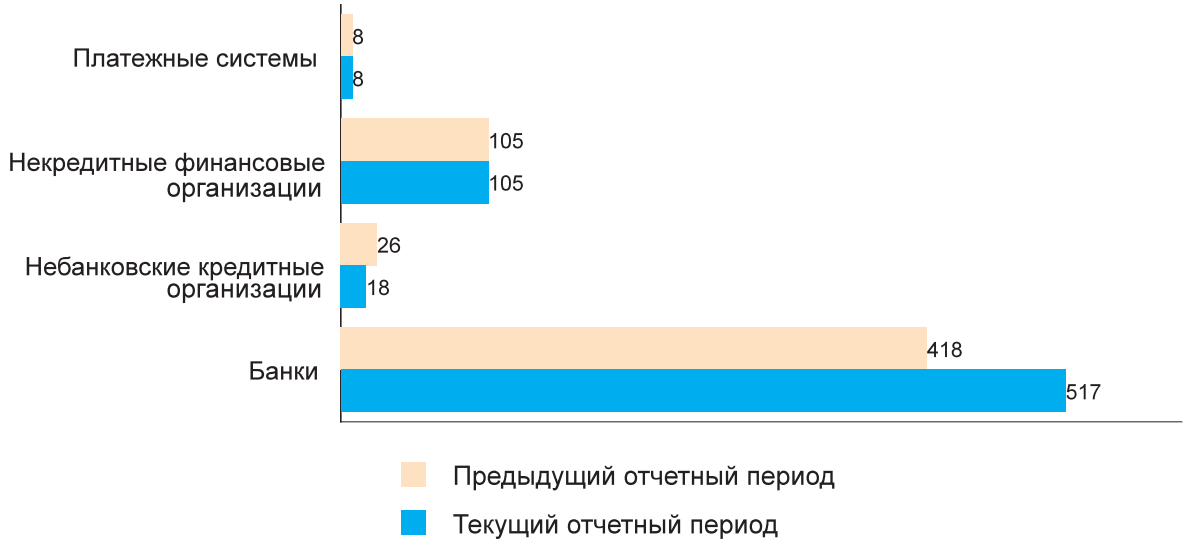
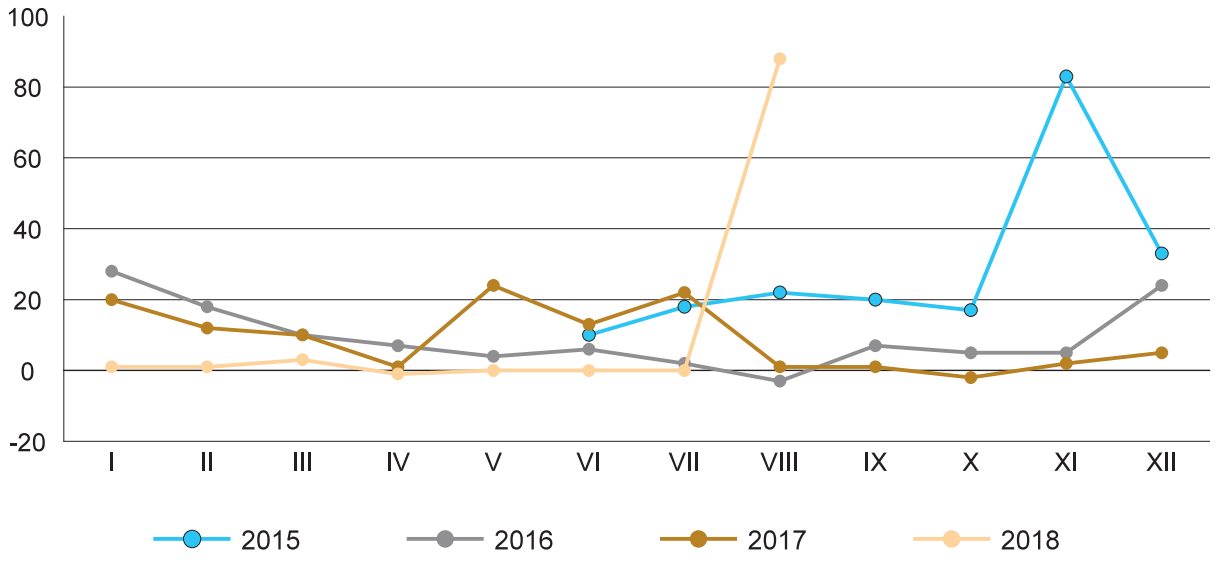


Рисунок 3
Динамика подключения банков



ге были приняты три взаимодополняющих правовых документа, которые не только создали нормативную основу для легализации обмена данными об инцидентах в электронных платежных системах, но и установили прямую обязанность финансовых организаций (в первую очередь кредитных) предоставлять такие данные в ФинЦЕРТ[1].

Принятие этих нормативных документов обусловило взрывной рост числа банков, участвующих в обмене.

При этом в целом в отчетный период динамика подключения новых организаций и увеличение количества направляемых в ФинЦЕРТ сообщений об инцидентах указывали на существенный рост активности участников информационного обмена. Это можно объяснить наглядной демонстрацией его практического значения для партнеров ФинЦЕРТ после массовых атак вирусов WannaCry, NotPetya и BadRabbit. Примечательно, что в целом банковский сектор от них практически не пострадал (за исключением нескольких заразившихся WannaCry банкоматов и одного терминала).

Так, в 2017 г. выявлено два ранее не типичных для этого времени года пика подключений – в мае и июле. Это совпадает с массовыми волнами рассылок вирусов WannaCry и NotPetya.

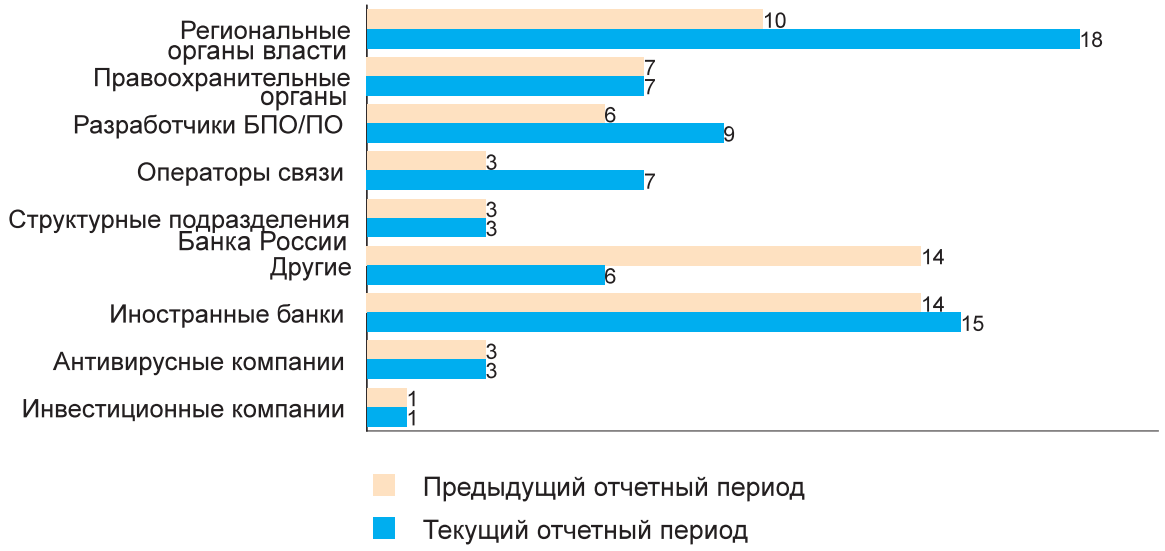
Информационный обмен с неподнадзорными организациями

Для неподнадзорных Банку России организаций участие в информационном обмене останется добровольным. ФинЦЕРТ взаимодействует с ними на основании соглашений о взаимодействии по вопросу противодействия компьютерным атакам.

ФинЦЕРТ постоянно ведет поиск новых источников информации по компьютерным атакам и угрозам, одновременно привлекая к инфор-

[1] *Федеральный закон № 167-ФЗ, Федеральный закон №187-ФЗ и новая редакция Положения Банка России № 382-П.*

Рисунок 4
Неподнадзорные организации – участники обмена



мационному обмену компании-интеграторы, разработчиков программного обеспечения, в том числе средств антивирусной защиты, провайдеров сети Интернет, операторов связи и представителей других государственных органов, курирующих информационную безопасность отрасли.

Международное сотрудничество

ФинЦЕРТ развивает взаимодействие с иностранными партнерами по двум основным направлениям: создание единого киберпространства и доверенной финансовой среды в рамках Евразийского экономического союза (ЕАЭС) и организация информационного обмена с национальными и международными организациями по обеспечению кибербезопансости.

Данные функции ФинЦЕРТ выполняет в рамках реализации задачи Банка России по обеспечению устойчивости финансовых организаций и доступности финансовых услуг в соответствии с Федеральным законом от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».

В рамках работы с ЕАЭС ФинЦЕРТ осуществляет консультационную и методологическую помощь национальным (центральным) банкам стран ЕАЭС по созданию собственных групп реагирования на компьютерные инциденты. В 2018 г. Банк России подписал соглашения о взаимодействии в области обеспечения информационной безопасности с Национальным банком Республики Казахстан, Центральным банком Республики Армения и Национальным банком Республики Беларусь. До конца 2018 г. планируется подписать аналогичное соглашение с Национальным банком Кыргызской Республики.

В перспективе Банк России рассматривает целесообразность аналогичной работы на пространстве БРИКС.

Задачами ФинЦЕРТ в области сотрудничества с международными и национальными организациями в области кибербезопасности являются взаимное информирование по компьютерным инцидентам и блокировка мошеннических информационных ресурсов.

Эта работа позволяет российским заинтересованным лицам получать оперативную информацию о компьютерных атаках на иностранные кредитные организации и устройства самообслуживания. Полученные от зарубежных партнеров данные ФинЦЕРТ использует для своевременного уведомления участников информационного обмена о резонансных и значимых компьютерных инцидентах и об актуальных угрозах.

В 2017 г. Банк России стал участником двух лидирующих международных организаций в сфере обеспечения информационной безопасности – FIRST и EAST EGAF. Наряду с обменом данными о киберугрозах специалисты обеих сторон совместно готовят расширенные информационные материалы. Так, за отчетный период ФинЦЕРТ совместно с EAST EGAF выпустил для своих партнеров три таких бюллетеня.

FIRST *(Forum for Incident Response and Security Teams – международное сообщество команд реагирования на инциденты)*

EAST EGAF *(European ATM Security Team – Expert Group on ATM Fraud – европейская команда – экспертная группа по противодействию мошенничеству, связанному с банкоматами)*

В частности, на основе данных, поступивших из стран ЕАЭС, о взломе банкоматов был проведен анализ ситуации и оперативно выпущены бюллетени, информация которых позволила предотвратить аналогичные покушения как в стране – источнике информации, так и в других странах ЕЭАС.

Информация, полученная из ЕАЭС, содержащая подробности рассылки фишинговых писем и ВПО, также помогла предотвратить распространение ВПО и предупредить покушения на хищение денежных средств всех участников обмена ввиду оперативного выпуска бюллетеня.

Помимо актуальной информации по киберугрозам, ФинЦЕРТ обменивается опытом работы в данной сфере с ведущими группами реагирования на компьютерные атаки (CERT) Испании, Болгарии, Японии, Швейцарии, Индии, Китая, США, Нидерландов, Великобритании, Панамы, Израиля.

Группы реагирования этих стран подтверждали наличие фактов, выявленных специалистами ФинЦЕРТ, и предотвращали финансовые потери и киберпреступления на территориях суверенных государств.

ИНФОРМИРОВАНИЕ УЧАСТНИКОВ ОБМЕНА

Активность участников обмена позволяет ФинЦЕРТ аккумулировать значительные объемы о информации о киберугрозах и кибератаках, подробно и детально изучать особенности каждого из показателей и своевременно оповещать своих партнеров об угрозах, предоставляя средства противодействия.

За прошлый отчетный период количество разосланных бюллетеней составило 211 штук.

Увеличение количества рассылок в периоды массовых атак вирусов WannaCry, NotPetya и BadRabbit свидетельствует о повышении качества мониторинга угроз и атак, а также о возросшей активности участников информационного обмена. Это в свою очередь позволяет повысить оперативность и качество информационного обмена и, как следствие, уровень защищенности участников экономической деятельности.

Рисунок 5
Количество разосланных бюллетеней

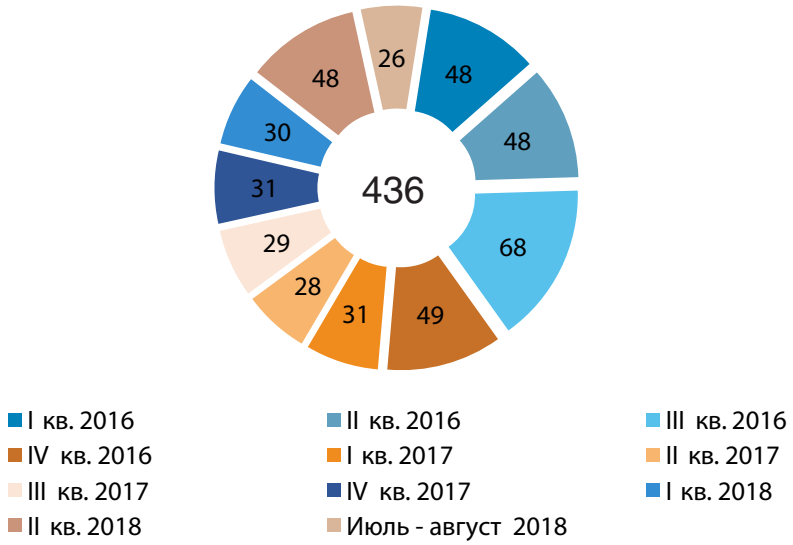
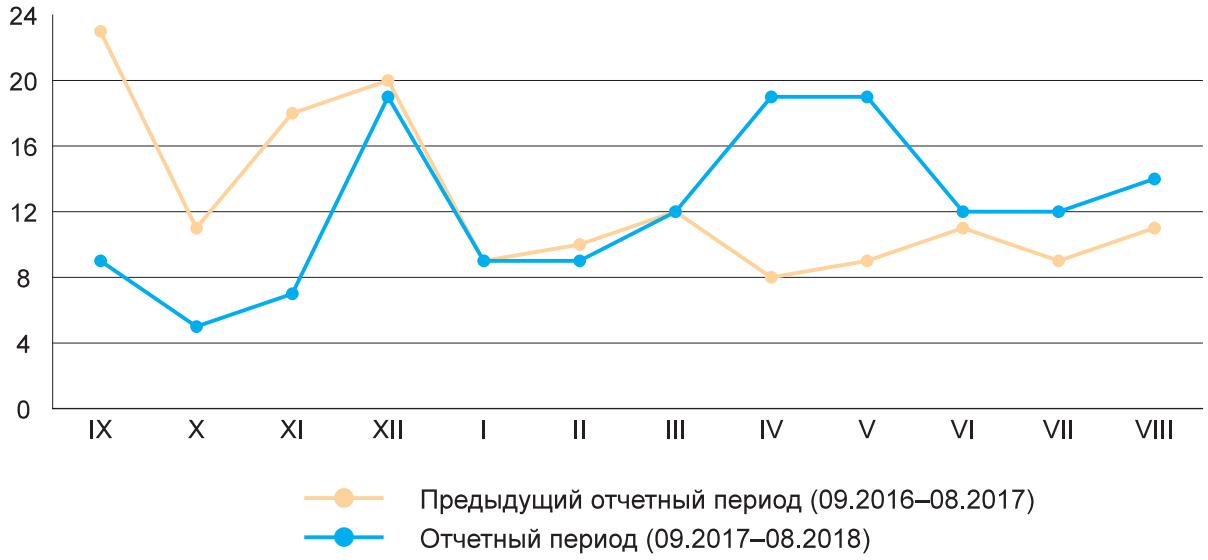


Рисунок 6
Информационные рассылки ФинЦЕРТ



Превращение информационного обмена из добровольной функции финансовых организаций в обязательную повлечет за собой увеличение числа сообщений о киберинцидентах, поступающих в ФинЦЕРТ, и повысит качество информации, получаемой об атаках, что, в свою очередь, позволит перейти к целевым уведомлениям со стороны ФинЦЕРТ. Расширение международного сотрудничества и рост количества участников обмена также могут стать факторами, способствующими увеличению числа направляемых участникам обмена информационных материалов.

АВТОМАТИЗАЦИЯ ИНФОРМАЦИОННОГО ОБМЕНА

Система АСОИ ФинЦЕРТ

Для упрощения процесса информационного обмена, а также повышения оперативности и уровня его защищенности ФинЦЕРТ создал автоматизированную систему обработки инцидентов (АСОИ ФинЦЕРТ). В настоящий момент к АСОИ ФинЦЕРТ подключились все банки Российской Федерации.

В июле 2018 г. введена в эксплуатацию первая очередь АСОИ, состоящая из информационного портала, сервиса личных кабинетов и специализированных технологических подсистем и защищенной инфраструктуры, что позволяет реализовать следующие процессы:

- получение данных от участника (информация об инцидентах в организации, выявленных уязвимостях, угрозах, данных о раскрытии информации, запросах);
- передача информации участнику и его оперативное информирование об актуальных угрозах информационной безопасности в кредитно-финансовой сфере (в том числе путем направления соответствующих бюллетеней);

- оперативное взаимодействие между участником и ФинЦЕРТ по инцидентам и запросам;
- мониторинг информационных атак на организации кредитно-финансовой сферы и поддержка взаимодействия ФинЦЕРТ с регистраторами и хостерами по инициации разделегирования/блокировки мошеннических и вредоносных ресурсов.

Использование участником информационного обмена АСОИ ФинЦЕРТ позволяет существенно облегчить выполнение требований Федерального закона № 187-ФЗ, Федерального закона № 167-ФЗ и положений Банка России № 382-П и № 552-П.

АСОИ ФинЦЕРТ поддерживает получение и прием информации от участников информационного обмена, передаваемую путем:

- заполнения интерактивных форм в личном кабинете;
- передачи информации в виде json-файлов, оформленных в соответствии с проектом стандарта «Технология подготовки, направления и формы электронных сообщений для информационного обмена с Банком России о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации»[2];
- передачи информации xlsx-файлов, соответствующих формам INT, EXT и PUB и их заполнению[3];
- в рамках централизованной базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента (АС «Фид-АнтиФрод»).

Система «Фид-АнтиФрод»

Система «Фид-АнтиФрод»
– инструмент обмена данными недобросовестных получателей платежей

Федеральный закон № 167-ФЗ предусматривает создание Банком России базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента и обеспечения возможности получения кредитными организациями данных из этой базы.

С этой целью Банк России создает систему «Фид-АнтиФрод», которая будет работать как самостоятельная система на основе АСОИ ФинЦЕРТ, используемой в качестве базовой инфраструктурно-технологической платформы.

Система «Фид-АнтиФрод» предназначена для аккумулирования и быстрого обмена информацией об операциях без согласия клиента. Основными участниками такого обмена станут операторы по переводу электронных денежных средств, операторы услуг платежной инфраструктуры и Банк России.

Информация об операциях без согласия клиента будет доводиться до участников информационного обмена в АСОИ ФинЦЕРТ через направление специальных сообщений, так называемых «фидов», которые будут содержать признаки операций, совершенных без согласия клиента.

Интуитивно понятный интерфейс позволит участникам информационного обмена вносить данные об операциях вручную без использования дополнительно установленного специального программного обеспече-

---

[2] По состоянию на 8.08.2018 проект стандарта проходит процедуру его оформления.

[3] Порядок заполнения информации об инцидентах приведен во Временном регламенте передачи данных участников информационного обмена в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (http://cbr.ru/StaticHtml/File/14408/inforegl_23.pdf). Формы INT, EXT и PUB опубликованы на сайте Банка России в разделе «ФинЦЕРТ», http://cbr.ru/fincert/.

ния. Наряду с этим банки получат описание программного интерфейса для интеграции своих информационных систем с АС «Фид-АнтиФрод», что позволит им формировать и направлять сообщения в систему в автоматическом режиме по мере обнаружения и регистрации инцидента в системах банка.

Система «Фид-АнтиФрод» позволит кредитным организациям дополнять свои антифрод-системы информацией, получаемой от других банков, уже столкнувшихся с мошенниками. Это существенно повысит эффективность работы по предотвращению хищений денежных средств со счетов клиентов.

РАБОТА С ОБЩЕСТВЕННОСТЬЮ

Рост числа жертв социальной инженерии, крупные хищения и резонансные кибератаки способствовали росту общественного интереса и социальной значимости темы информационной безопасности финансового сектора. Развитие нормативного регулирования работы участников рынка по противодействию мошенникам на фоне появления и внедрения новых финансовых технологий обусловило необходимость освещения этой деятельности в средствах массовой информации.

Кризисные коммуникации ФинЦЕРТ строятся в двух направлениях. В первую очередь это упреждающие, превентивные меры, направленные на снижение числа успешных кибератак. Как показывает практика, применение федеральных законов и нормативных документов Банка России вызывает со стороны профессионального сообщества потребность в разъяснительной работе по отдельным вопросам. ФинЦЕРТ отвечает на них в рамках крупнейших отраслевых форумов – Finopolis 2017, Soc Forum, Antifraud Russia 2017, Уральского форума по информационной безопасности, ITSF, МФК-2017. Помимо этого, специалисты ФинЦЕРТ регулярно выступают с докладами на тематических мероприятиях и участвуют в дис-

Рисунок 7
Публикации в СМИ*

** На основе данных Скан-Интерфакс.*

куссиях с представителями служб информационной безопасности финансовых организаций.

Другим направлением превентивной работы ФинЦЕРТ является борьба с «социальной инженерией». Для этого ФинЦЕРТ участвует в программах по повышению финансовой и киберграмотности населения, тематических публикациях в средствах массовой информации и общественных лекциях.

Второй блок коммуникаций ФинЦЕРТ связан с минимизацией последствий уже случившихся киберинцидентов. Так, появление в прессе и соцмедиа информации о хищениях в кредитных организациях является фактором риска для их финансовой стабильности. ФинЦерт снижает этот риск путем корректной и своевременной подготовки комментариев для СМИ, разъясняющих действия банка и регулятора по минимизации последствий инцидентов и снижению вероятности их повторения в других банках.

Наиболее цитируемые темы:
- *более 1 млрд руб. похитили хакеры у российских банков*
- *кибератаку на «ПИР банк» совершили хакеры из Carbanak*
- *Банк России обязал банки информировать его о хакерских атаках*
- *художественная подсветка к ЧМ-2018 украсила ростовскую телебашню*
- *Банк России обязал банки сообщать о полученном спаме*
- *в Банке России сообщили о блокировке более 600 мошеннических сайтов*
- *зафиксирован рост числа взломов банкоматов с помощью технологии blackbox*
- *Банк России обяжет банки обмениваться информацией с ФинЦЕРТ*

Мониторинг сообщений о работе финансовых организаций в публичном интернет-пространстве

ФинЦЕРТ на постоянной основе проводит мониторинг открытых ресурсов сети Интернет для обнаружения и предупреждения информационных атак на организации кредитно-финансовой сферы, угрожающих ее стабильности. Для этого ФинЦЕРТ использует специализированную систему анализа социальных медиа и средств массовой информации, которая ежедневно индексирует около 200 000 текстовых и графических публикаций по более чем 200 выделенным объектам (темам) кредитно-финансовой сферы.

Источниками информации для анализа являются более 100 000 различных интернет-ресурсов, среди которых популярные электронные СМИ, тематические СМИ финансового сектора, форумы, популярные социальные сети, блоги, микроблоги, видеохостинги, каналы и группы в мессенджерах WhatsApp и Telegram и многие другие.

Все проиндексированные сообщения проходят процесс автоматического распределения по темам мониторинга, им присваиваются такие атрибуты, как тональность, регион публикации, автор, тематика, количественные показатели по распространению, просмотрам, «лайкам», «репостам» и прочее.

Исследуя весь этот массив в автоматическом, а также ручном режиме, специалисты ФинЦЕРТ определяют как естественные всплески интереса к кредитно-финансовым организациям, так и возможные целенаправленные информационные атаки на них. Если обнаруживается какая-либо аномалия, проводится тщательный анализ всего массива связанных материалов, изучаются их авторы. Это дает понимание, насколько чувствительна тема, кто о ней пишет и сложилась ли реальная критическая ситуация, требующая внимания регулятора. Имеет ли место естественное распространение информации, пусть даже из категории слухов, или произведен вброс, распространяется так называемый «фейк».

Детектируя аномальный всплеск активности, ФинЦЕРТ изучает причины его возникновения и подробности, фактуру темы. Если интерес со стороны пользователей реальный, тема набирает обороты – лайки, перепосты, комментарии – информируется руководство и, если необходимо, ФинЦЕРТ принимает участие в выработке мер реагирования, в том

числе предусматривающих выпуск официальных разъяснений пресс-службы Банка России.

В период с августа 2017 г. по август 2018 г. было тщательно исследовано более 80 таких аномальных информационных событий в информационном поле кредитно-финансовой сферы.

Повышение киберграмотности и киберкультуры

ФинЦЕРТ участвует в системной работе Банка России по повышению финансовой и киберграмотности населения. Сегодня в ряде банков действуют аналогичные программы для клиентов, и ФинЦЕРТ может стать центральным звеном, своего рода информационно-координационным хабом всех процессов по повышению киберграмотности населения. В этом случае можно рассчитывать на синергию усилий и возможностей участников рынка и регулятора и, как следствие, на реальное снижение ущерба от действий киберпреступников.

Практическая реализация этих задач планируется путем создания и использования оперативно адаптируемой к новым методам и приемам «социальной инженерии» системы мероприятий по реагированию и оповещению о них ключевых целевых групп населения.

Снижение уязвимости целевых групп населения к приемам «социальной инженерии» позволит снизить число несанкционированных переводов и объем ущерба от них и, как следствие, повысить доверие населения к кредитно-финансовой системе и ее устойчивость.

Текущие проекты

Профилактика среди школьников

Чтобы школьники как можно реже становились жертвами мошенников, ФинЦЕРТ проводит для них просветительские семинары о безопасности платежных услуг и кибербезопасности в целом. Так, в 2018 г. в рамках городского проекта «Школы новых технологий» при поддержке Департамента ИТ Москвы стартовал цикл таких мероприятий для школьников 6–8 классов. Также ФинЦЕРТ примет участие в организации и проведении диктанта по киберграмотности, который пройдет на базе детских библиотек по всей России по инициативе Российской государственной детской библиотеки.

Работа с профессионально ориентированными аудиториями

В 2018 г. ФинЦЕРТ принял участие в проведении Всероссийского конкурса научно-технологических проектов «Большие вызовы» под эгидой образовательного центра «Сириус». Вместе со специалистами ФинЦЕРТ команда участников конкурса, состоявшая из школьников 8–11 классов, разработала программный комплекс для автоматизации выявления индикаторов компрометации, полученных участниками информационного обмена, который получил высокую оценку от жюри конкурса и организаторов мероприятия. Сейчас ФинЦЕРТ ведет переговоры с руководством «Сириуса» о создании на площадке учебного центра образовательного киберполигона для непрерывного обучения талантливых ребят.

Работа со студентами планируется в форме лекций на площадках Московского политехнического университета (МосПолитех) и Московского финансово-юридического университета (МФЮА). ФинЦЕРТ готов рассматривать сотрудничество со студентами ВУЗов через проектную деятельность как по вопросам финансовой ИТ и кибербезопасности, так и по решению конкретных практических задач в области функционала ФинЦЕРТ. Лучшие из них смогут пройти практику в Банке России с возможным последующим трудоустройством.

Еще одно направление работы с профессиональной аудиторией – это обучение сотрудников правоохранительных органов и участие в учебных семинарах по вопросам информационной безопасности. В августе этого года ФинЦЕРТ пригласил на стажировку представителей национальных банков стран – участников ЕАЭС, с которыми поделился опытом создания центров реагирования на компьютерные инциденты.

Обучаем тех, кто учит

Школьные учителя по-прежнему остаются одними из тех, кто может научить подростков азам киберграмотности и «цифровой гигиены». Поэтому для них ФинЦЕРТ разрабатывает методические материалы и проводит обучающие мероприятия.

Одним из крупнейших проектов стал открытый урок по теме «Киберпреступления», который сотрудники ФинЦЕРТ провели совместно с издательством «Просвещение» в феврале 2018 года. Трансляция велась через телемост на все субъекты Российской Федерации.

Наряду с этим ФинЦЕРТ разрабатывает программы учебных курсов по безопасности платежных услуг для различных слоев населения. К разработке учебных материалов для школьников и студентов ФинЦЕРТ привлекает коллег из других подразделений Банка России. Параллельно разрабатываются материалы по киберграмотности для портала fincult.info.

Публичные лекции

ФинЦЕРТ принимает участие в мероприятиях других организаций, для которых очевидна актуальность повышения киберграмотности населения. В 2017 г. специалисты ФинЦЕРТ приняли участие в работе «Школы кибербезопасности», организованной Московским Политехом и Открытым университетом Сколково. Программа Школы включала лекции, мастер-классы и практические занятия. Специалисты ФинЦЕРТ рассказали слушателям о трендах рынка информационной безопасности финансового сектора, работе ФинЦЕРТ и перспективных направлениях развития карьеры в этой области.

В мае 2018 г. сотрудники ФинЦЕРТ выступили перед участниками IV Всероссийского конгресса волонтеров финансового просвещения. Информация, полученная делегатами конгресса, позволит им интегрировать направление киберграмотности в тему финансового просвещения, объединив усилия по защите граждан Российской Федерации в сфере финансовых услуг.

ВЫВОДЫ И ПРОГНОЗЫ

В дальнейшем по мере распространения требований Федерального закона № 167-ФЗ на некредитные финансовые организации ожидается дальнейшее увеличение числа участников информационного обмена из числа поднадзорных Банку России (микрофинансовые и страховые организации, пенсионные фонды и другие – всего более 20 тысяч). На них, как сейчас на кредитные организации, будет возлагаться обязанность по незамедлительному информированию Банка России о компьютерных инцидентах.

В свете указанных нормативных изменений все поднадзорные организации обязаны будут подключиться к информационному обмену ФинЦЕРТ. Такое подключение будет происходить постепенно по мере увеличения технологических мощностей АСОИ ФинЦЕРТ.

Динамика участия в информационном обмене неподнадзорных организаций зависит от внешних факторов, среди которых прежде всего нужно назвать число успешных компьютерных атак (как следствие разработки новых ВПО) и несанкционированных операций по переводу денежных средств как физических, так и юридических лиц. Однако с запуском системы «Фид-АнтиФрод» ожидается существенное снижение их числа, что, скорее всего, несколько замедлит динамику подключения неподнадзорных организаций. Влияние этого фактора может быть компенсировано повышением качества информации, получаемой об атаках от финансовых организаций после вступления в силу Федерального закона № 167-ФЗ, и переходом к целевым уведомлениям участников обмена.

Также необходимо учитывать, что компьютерные атаки носят трансграничный характер (например, тестирование новых видов компьютерных атак может проходить в одних странах, а последующее их широкомасштабное применение – в других). В связи с этим особое значение приобретает информационное взаимодействие с иностранными организациями, специализирующимися на оказании услуг в области обеспечения информационной безопасности. Поэтому ФинЦЕРТ планирует расширять круг иностранных партнеров, изучать международный опыт функционировании CERT и реализовать лучшие международные практики информационного обмена в сфере кибербезопасности.

В рамках реализации Федерального закона № 167-ФЗ банки должны в обязательном порядке сообщать в ФинЦЕРТ о намерении раскрыть информацию об инцидентах на официальных сайтах в сети Интернет, в пресс-релизах, на пресс-конференциях. ФинЦЕРТ будет получать эту информацию не позднее одного рабочего дня до раскрытия и готовить материалы для подготовки официальных комментариев Пресс-службой Банка России.

2. Инциденты информационной безопасности в кредитно-финансовой сфере

НУЛЕВЫЕ ПОТЕРИ БАНКОВ И ИХ КЛИЕНТОВ В ХОДЕ ЧМ-2018

Массовые мероприятия всегда привлекают интерес мошенников (вспомним Олимпиаду-2014). В преддверии Чемпионата мира по футболу FIFA 2018 (ЧМ-2018) специалисты ФинЦЕРТ проанализировали потенциальные риски и провели с участниками кредитно-финансовой сферы ряд подготовительных мероприятий.

ФинЦЕРТ разработал рекомендации[1] по защите объектов информационной инфраструктуры и противодействию атакам на устройства банковского самообслуживания и платежные терминалы. Кредитные организации провели работы по реализации указанных в них превентивных мер и сообщили о готовности инфраструктуры и персонала к возможным нештатным ситуациям.

Кроме этого, было заключено Соглашение с FIFA о мероприятиях, направленных на защиту бренда FIFA в кредитно-финансовой сфере.

В период ЧМ-2018 ФинЦЕРТ зафиксировал:

- девять попыток хищения денежных средств из банкоматов кредитных организаций с использованием устройств типа blackbox;
- две массовые рассылки писем-угроз якобы от хакерских группировок с требованием уплаты выкупа за неосуществление атаки;
- 19 массовых рассылок вредоносного программного обеспечения;
- три DDoS-атаки мощностью до 991,7 Мбит/с.

Применение предложенных ФинЦЕРТ мер свело к нулю потери организаций кредитно-финансовой сферы от перечисленных атак. Полученная по результатам детального анализа инцидентов информация доведена до участников информационного обмена ФинЦЕРТ, правоохранительных органов и координационных центров по администрированию доменов.

[1] *Опубликованы в разделе «ФинЦЕРТ» на официальном сайте Банка России, www.cbr.ru/fincert.*

Совместная работа участников кредитно-финансовой сферы и ФинЦЕРТ помогла избежать нештатных ситуаций и создать максимально комфортные условия для проведения ЧМ-2018 для граждан России и иностранных гостей.

ВРЕДОНОСНЫЕ САЙТЫ, СМС-РАССЫЛКИ И КОЛЛ-ЦЕНТРЫ МОШЕННИЧЕСКИХ СТРУКТУР

Уровень грамотности россиян в сфере информационной безопасности позволяет мошенникам из года в год успешно использовать информационные технологии и средства связи в сочетании с приемами так называемой «социальной инженерии» (злонамерное введение в заблуждение путем обмана или злоупотребления доверием) для хищения средств с их личных счетов или счетов их работодателей. Так, в 2017 г. мошенники похитили у физлиц более 1 млрд рублей.

При этом различные социальные категории граждан подвержены разным типам воздействия. Конечной целью злоумышленников является перевод средств жертв на их счета, но средства ее достижения варьируются. С одними связываются по телефону напрямую или через СМС и вынуждают совершать операции по переводу самостоятельно. Для других достаточно организовать веерную рассылку писем с текстом, побуждающим открыть файл с вирусом или пройти по ссылке на зараженный сайт, и таким образом буквально «открыть» злоумышленникам доступ к управлению счетами физлица или организации через системы дистанционного банковского обслуживания. Третьих привлекают скидки и бонусы при покупке, как выясняется впоследствии, несуществующих товаров в мошеннических интернет-магазинах (фишинг).

Противодействие таким преступлениям – одно из целевых направлений работы ФинЦЕРТ. Прекращение работы мошеннических колл-центров и блокировка СМС-рассылок происходит при участии операторов связи и телеком-провайдеров. Для борьбы с фишингом у Банка России в лице ФинЦЕРТ есть полномочия по инициированию снятия с делегирования мошеннических интернет-ресурсов. При обнаружении сайтов с вредоносным программным обеспечением ФинЦЕРТ направляет информацию о них в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

***01.2017 – 08.2017**:*
- *разделегировано 367 доменов (из 481 предложенного);*

***09.2017 – 08.2018**:*
- *разделегировано 1668 доменов (из 2205 предложенных)*

ФинЦЕРТ начал блокировать фишинговые ресурсы с января 2017 года.

Борьба с СМС-рассылками и колл-центрами мошеннических структур

В настоящее время в информационном обмене с ФинЦЕРТ участвуют четыре оператора связи. В рамках взаимодействия с ними ФинЦЕРТ направил на блокировку 127 номеров мобильных операторов и номеров в коде 8–800, а также более 100 массовых мошеннических СМС-рассылок.

ФинЦЕРТ планирует усилить работу по блокировке сайтов, рассылок и колл-центров мошеннических структур. Предполагается наладить взаимодействие с операторами не только мобильной связи и телеком-провайдерами, но и ip-телефонии и мессенджеров, а также развивать взаимодействие с профильными государственными органами.

Сайты с ВПО

Как и в предыдущие годы, одним из основных инструментов компьютерных преступников является вредоносное программное обеспечение. Спам-рассылки писем с зараженными вирусами файлами или ссылками на сайты с ВПО активно используются для атак на финансовые организации и их клиентов.

Информацию о выявленных доменах, которые содержат вредоносное программное обеспечение, ФинЦЕРТ направляет в антивирусные лаборатории, поисковые системы и разработчикам браузерных решений. Они,

Рисунок 8
Основные типы ВПО

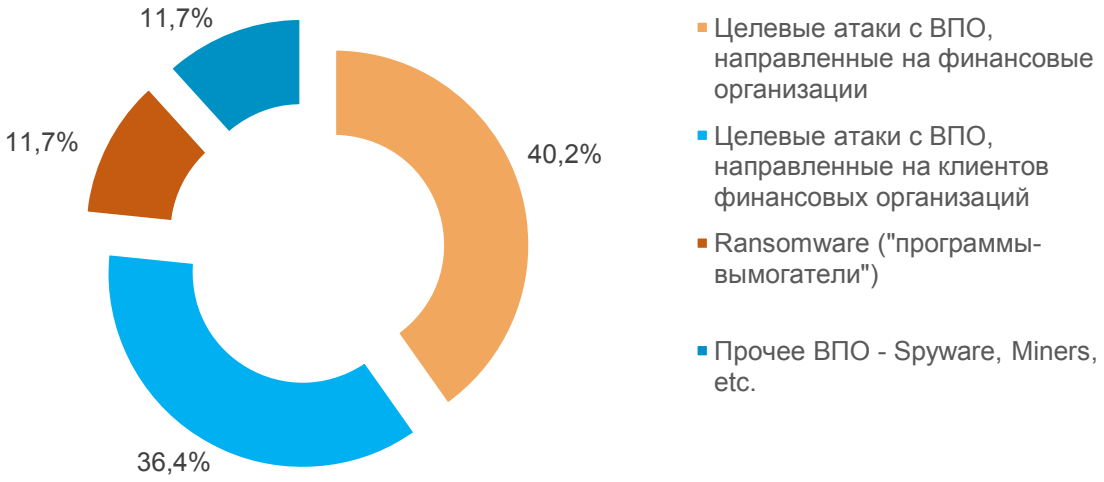
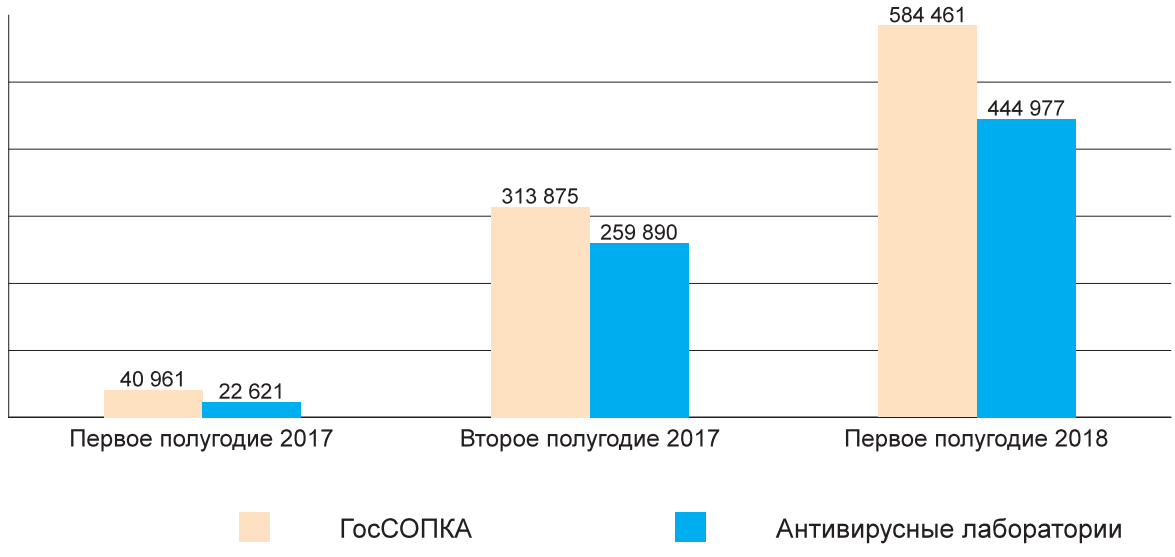


Рисунок 9
Выявленные домены с ВПО



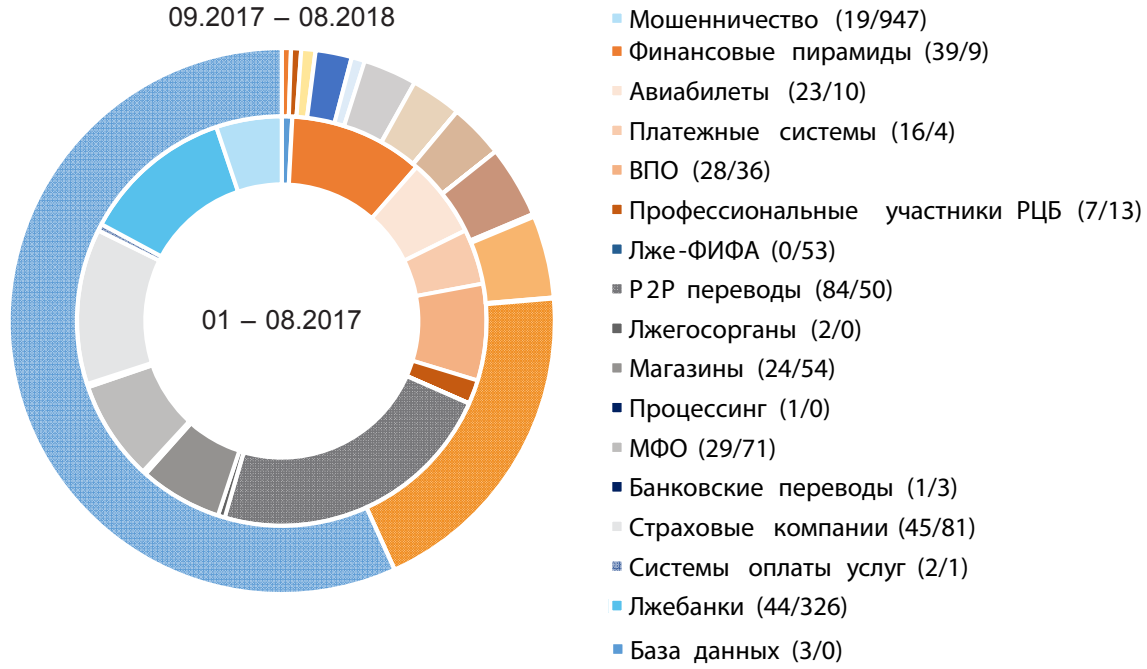
в свою очередь, формируют и корректируют свои базы. Аналогичные сотрудничество происходит и с ГосСОПКА, активно использующей полученные данные в своей работе.

Начиная с сентября 2017 г. ФинЦЕРТ самостоятельно инициировал снятие с делегирования 38 ресурсов, распространяющих вредоносное программное обеспечение.

Снятие с делегирования фишинговых сайтов

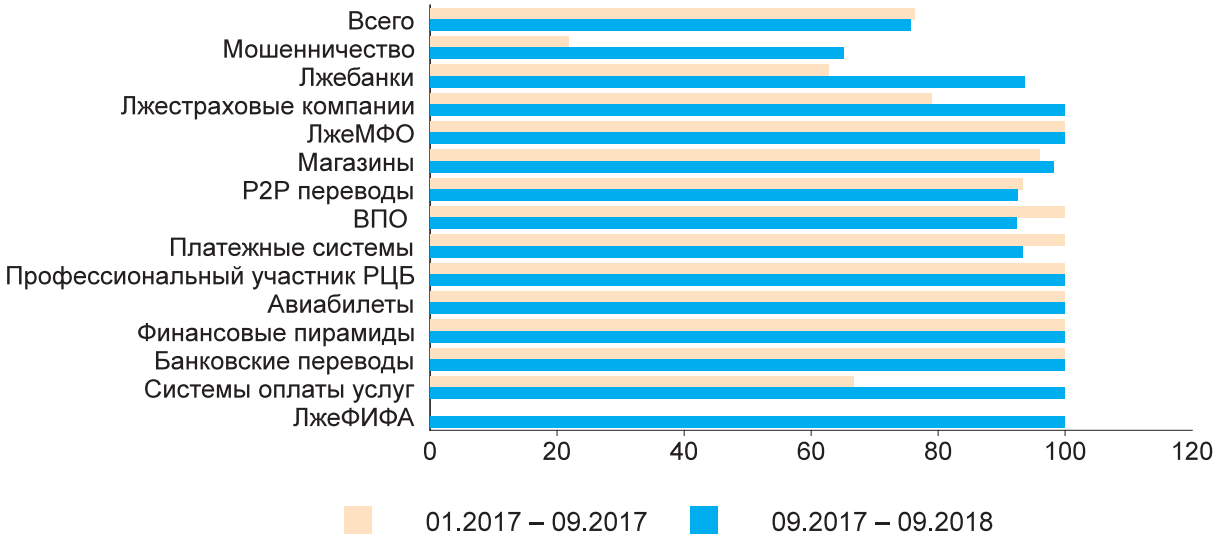
За отчетный период ФинЦЕРТ инициировал снятие с делегирования 1668 фишинговых доменов. Наибольшее число из них приходится на мошеннические сайты, сайты компаний, не имеющих лицензии Банка России на оказание предлагаемых финансовых услуг, лжебанков, МФО и мошеннических страховых компаний, а также мошеннические сайты по продаже билетов на матчи проходившего на территории России Чемпионата мира по футболу 2018 г. (группа лжеФИФА).

Рисунок 10
Разделегированные домены



По сравнению с прошлым отчетным периодом виден сохранившийся основной тренд – это рост интернет-мошенничества. Также почти в 8 раз выросло число блокируемых сайтов лжебанков, в 2–2,5 раза – МФО и интернет-магазинов. В 1,8 раз увеличилось число заблокированных сайтов мошеннических страховых компаний. Рост числа последних, вероятно, связан с введением электронного ОСАГО.

Рисунок 11
Доля снятых с делегирования доменов (%)



Постепенный уход с линии лидеров мошеннических P2P переводов и финансовых пирамид мы объясняем эффектом проводимой ФинЦЕРТ работы по повышению киберграмотности населения, а также борьбы с самими пирамидами.

Как и в предыдущем отчетном периоде, положительное решение о разделегировании принимается примерно в 76% случаев, то есть по каждым трем из четырех доменов, предлагаемых ФинЦЕРТ. Однако проводить прямую параллель не совсем корректно: в прошлом периоде направляемых на разделегирование сайтов было в 4,5 раз меньше, при этом доля мошеннических ресурсов, составляющих сейчас более половины всех блокируемых, тогда не превышала 6%. При почти 50-кратном росте их количества доля разделегированных увеличилась – с 21% в прошлом отчетном периоде до 65% в этом. Также на треть выросла доля разделегируемых сайтов лжебанков и мошеннических страховых компаний, составляющих вместе с мошенническими ресурсами более 3/4 фишинговых сайтов. Все это говорит о высоком качестве экспертизы ФинЦЕРТ при оценке мошеннических ресурсов.

По мнению ФинЦЕРТ, трендом следующего года станет дальнейший рост мошенических доменов, относящихся к категориям «лжебанки», «лжестраховые компании» и «лжеМФО». Помимо этого, если принять во внимание работу ФинЦЕРТ, проводимую по борьбе с мошенническими ресурсами в российских доменных зонах, **ожидается постепенный переход таких ресурсов в юрисдикцию иностранных доменных зон.**

Как происходит разделегирование

ФинЦЕРТ инициирует блокировку сайтов в рамках соглашений, подписанных с организациями, координирующими функции по администрированию и регламентированию работы ресурсов более чем в 80 доменных зонах и геодоменах. На данный момент это Координационный центр национального домена сети Интернет, Фонд Развития Интернет, MSK-IX, Фонд содействия развитию технологий и инфраструктуры Интернета.

Разделегирование доменов занимает в среднем от 1 до 3 дней

ФинЦЕРТ получает информацию о мошеннических ресурсах из разных источников: самостоятельного мониторинга, от поднадзорных организаций Банка России, правоохранительных и контролирующих органов, общественных организаций и граждан.

Процесс по разделегированию в ФинЦЕРТ выглядит следующим образом:

1. ФинЦЕРТ оценивает доказательственную базу и формирует комплексное заключение для регистратора о снятии ресурса с делегирования.

При определении фишингового ресурса ФинЦЕРТ руководствуется следующими критериями:

– отсутствие лицензии у организации, осуществляющей продажу товаров или оказание лицензируемых услуг;
– отсутствие информации об организации, предоставляющей услуги или осуществляющей продажу товаров, в справочниках и реестрах Банка России или уполномоченных органов государственной власти;
– ресурс не является официальным и не имеет никакого отношения к организации (критерий применяется только при непосредственном обращении организации);
– при перечислении денежных средств в счет оплаты оформленного заказа платеж осуществляется в пользу третьего лица (таким образом, отсутствует возможность предоставления дополнительных идентифицирующих сведений платежа, что затрудняет персонификацию оплаты товара).

Разработанные критерии в совокупности с мотивированным заключением позволяют практически безошибочно (99%) выявлять мошеннический ресурс.

2. Информация направляется в соответствующий координационный центр для принятия решения о разделегировании и последующих действий по блокировке домена.

3. После разделегирования домена ФинЦЕРТ направляет необходимую информацию в поисковые системы и разрабочикам браузерных решений для удаления ресурса из поисковой выдачи.

Запросы на разделегирование фишинговых ресурсов, в отношении которых у ФинЦЕРТ нет соответствующих компетенций (ресурс находится вне доменной зоны, где ФинЦЕРТ является компетентной организацией), направляются в Генеральную прокуратуру Российской Федерации, которая, в свою очередь, выносит постановление о возбуждении административного производства о признании информации запрещенной к распространению на территории Российской Федерации и направляет их в суд.

ТЕХНИЧЕСКИЙ АНАЛИЗ КОМПЬЮТЕРНЫХ АТАК

Технический анализ данных, поступающих от участников информационного обмена, является отдельным направлением в работе ФинЦЕРТ. Важным источником сведений об атаках является участие экспертов ФинЦЕРТ в проведении криминалистических исследований образцов вредоносного кода и носителей информации, пострадавших от воздействия таких кодов и других видов компьютерных атак.

Исследования проводятся на основании официальных запросов правоохранительных органов. В некоторых случаях специалисты ФинЦЕРТ

выезжают в кредитные организации для оказания помощи в сборе и фиксировании криминалистически важных объектов и первичного определения объектов, где могут находиться цифровые доказательства.

Такая деятельность позволяет детально изучить механизмы компьютерных преступлений против финансовых организаций и их клиентов.

По результатам технического анализа за отчетный период ФинЦЕРТ зафиксировал следующие наиболее часто встречающиеся типы компьютерных атак:

– целевые атаки на организации кредитно-финансовой сферы;
– атаки на граждан – клиентов кредитно-финансовых организаций при помощи методов социальной инженерии;
– нецелевые (спам-атаки) на организации кредитно-финансовой сферы;
– атаки на устройства самообслуживания;
– атаки на клиентов кредитно-финансовых организаций с использованием ВПО;
– атаки watering hole через зараженные популярные сайты, преимущественно СМИ. Данный вид атак направлен на посетителей сайтов, основная цель – получение удаленного доступа к компьютеру жертвы и поиск на нем интересующих данных (в частности, ДБО).

ЦЕЛЕВЫЕ АТАКИ НА ОРГАНИЗАЦИИ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ

Целевые атаки:
75% – различные виды майнеров
15% – письма различного фишингового содержания
10% – различные рекламные письма и письма-угрозы

Основываясь на результатах анализа, ФинЦЕРТ выявил три основных тренда.

1. Общий рост числа попыток атак, характеризовавшийся увеличением объема фишинговых писем, использованием незакрытых уязвимостей популярных веб-фреймворков, количеством попыток взлома инфраструктуры кредитных организаций через так называемые «бруты» – подбор учетных данных к доступным из сети Интернет элементам инфраструктуры, и так далее. Так, за I–II квартал 2017 г. было зафиксировано 39 целевых атак, за 8 месяцев ФинЦЕРТ выполнил рассылку 79 бюллетеней. За аналогичный период 2018 г. – 72 целевых атаки и 106 бюллетеней.

2. Доля успешных атак среди них, наоборот, снижается – как и ущерб от них по сравнению с аналогичным отчетным периодом. Это объясняется как деятельностью различных CERT, так и повышением общего уровня кибербезопасности организаций кредитно-финансовой сферы: значительная часть фишинговых писем отфильтровывается на почтовом шлюзе и иными компонентами систем защит, в результате чего вредоносное письмо не доходит до получателя. Данные выводы подтверждает и статистика ФинЦЕРТ: за 8 месяцев 2017 г. кредитные организации потеряли 1 078 762 345 руб., а за аналогичный период 2018 г. – 76 495 882 рублей. Количество успешных атак – 22 и 20 случаев соответственно.

3. Вектор интереса преступников смещается в сторону клиентов кредитных организаций – юридических лиц. Об этом свидетельствует рост числа попыток хищений именно у них. Так, ФинЦЕРТ наблюдал значительное количество атак, направленных на юридические лица, с использованием ВПО семейства Dimnie, оснащенного специальными модулями для работы с ДБО, а также ВПО семейства RTM. Так, за 8 месяцев года подготовлены и направлены участникам информационного обмена опера-

тивные бюллетени о 26 зафиксированных кампаниях распространения Dimnie и 10 кампаниях распространения RTM. Рост интереса злоумышленников к юридическим лицам можно объяснить как более слабой защитой малого и среднего бизнеса, так и вводом в действие законодательных актов, защищающих крупные организации, относящиеся к критической инфраструктуре Российской Федерации и ужесточающие наказание за атаки на них[2].

В дальнейшем, по мнению ФинЦЕРТ, общий тренд на снижение количества успешно осуществляемых крупных хищений непосредственно у кредитно-финансовых организаций сохранится. А число хищений у клиентов банков – юридических лиц и индивидуальных предпринимателей, наоборот, может возрасти. Одной из причин может стать произошедшие в текущем отчетном периоде утечки в Интернет исходного программного кода соответствующего ВПО, используемого для таких хищений.

Причины снижения ущерба

Определенное влияние на ситуацию оказало задержание в марте текущего года в Испании одного из руководителей группы киберпреступников, известной в публичных источниках как Cobalt Group (Cobalt Gang). Тем не менее атаки с использованием программного обеспечения Cobalt Strike после задержания не прекратились – группа продолжает свою деятельность. Необходимо отметить, что предположительно данная группа (либо значительная часть ее членов) ранее была известна как Carbanak и использовала одноименное ВПО.

[2] *По которым организации кредитно-финансовой сферы могут стать субъектами критической информационной инфраструктуры, атаки на которых, как предполагают злоумышленники, могут обойтись «дороже» – будет проводиться более тщательное расследование, к которому будут привлекаться высококвалифицированные специалисты и наказание может быть более суровым.*

За отчетный период ФинЦЕРТ зафиксировал три основных типа целевых атак, которые категорируются по используемым инструментам: Cobalt Strike/Carbanak, Silence и Dimnie.

Cobalt Strike/Carbanak

Группа проникает в организации кредитно-финансовой сферы, используя в большинстве случаев фишинговые письма, иногда «сбрученные» учетные данные. Для контроля над инфраструктурой используется легальное ПО для проведения тестирования на проникновение Cobalt Strike. Обычно конечная цель атаки – проникновение на банкоматы кредитной организации. Но иногда встречаются случаи с подменой информации в процессинге кредитной организации или с использованием системы международных переводов SWIFT. Общая схема атаки не претерпела принципиальных изменений и приведена на рисунках 12 (конечная цель – процессинг и 13 (конечная цель – банкомат).

Рисунок 12
Атака Cobalt Strike, конечная цель – процессинг

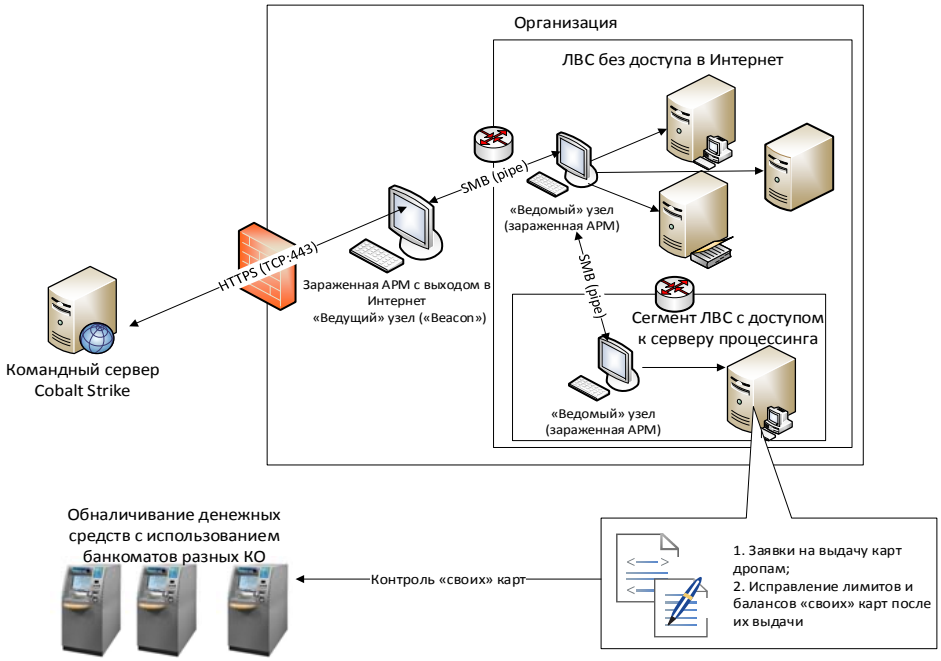
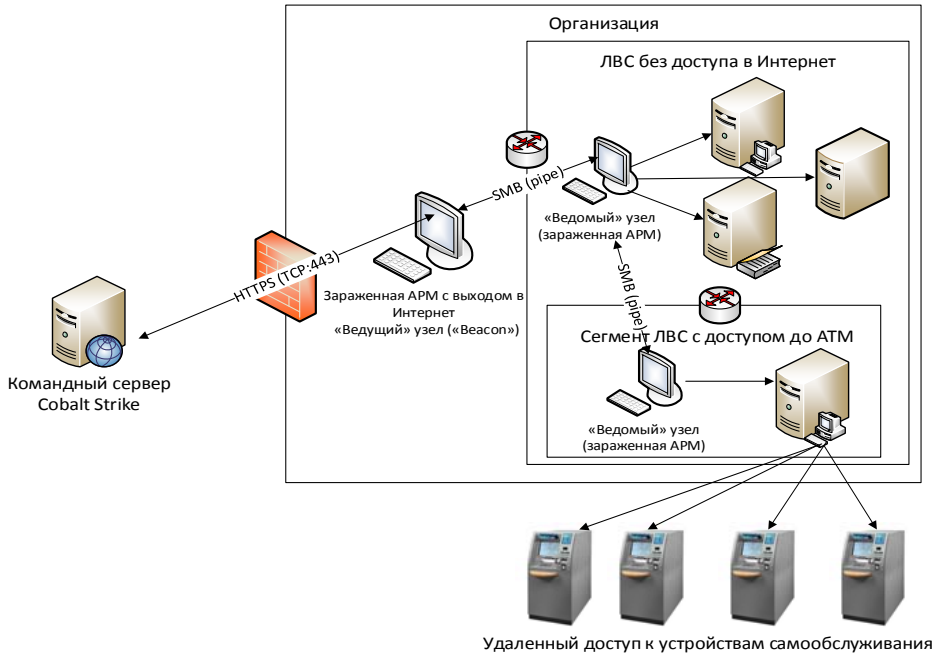


Рисунок 13
Атака Cobalt Strike, конечная цель – банкомат



Silence

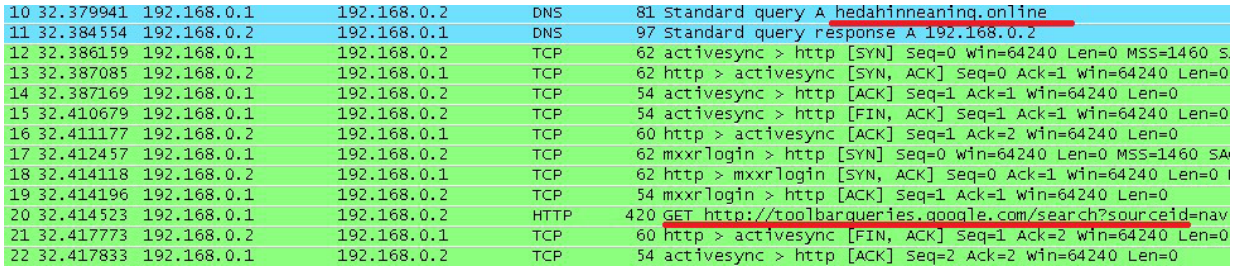
Впервые эти специфические инструменты зафиксированы в апреле 2017 г. (на протяжении 2017–2018 гг. было как минимум пять попыток атак, из которых две оказались успешными). Они применяются достаточно редко, что затрудняет его изучение.

Dimnie

Этот банковский троян изучен хорошо – за свою историю он прошел несколько крупных стадий развития: от троянской программы – «швейцарского ножа» для проникновения в компьютерные системы и хищения информации без более узкой специализации – до ВПО, применяющегося в основном для хищения денежных средств. Одной из характерных особенностей ВПО данного семейства является маскировка сетевых запросов под запросы к сервисам одного из гигантов интернет-индустрии (рисунок 14). «Финансовая» специализация Dimnie появилась с разработкой неустановленным лицом модуля, позволяющего совершать хищения как используя ДБО юридических лиц, так и посредством возможных атак на «старое» АРМ КБР (автоматизированное рабочее место клиента Банка России).

Другие группы, упоминаемые некоторыми исследователями, например Money Taker, якобы ориентированые на АРМ КБР, специалистами ФинЦЕРТ не встречались. Вместе с тем существует некоторое количество условно неклассифицированных атак, которые объединяет использование специального дистрибутива для проведения тестирования на проникновение – Kali Linux – «в чистом виде», то есть «из коробки». Возможно, именно эти атаки были совершены упомянутыми группами.

Рисунок 14
Сетевые запросы ВПО «Dimnie»



Общий тренд 2018 г., который, как полагают специалисты ФинЦЕРТ, распространится и на 2019 г. – снижение квалификации атакующих за счет все более массового использования общедоступных инструментов. Эти инструменты, созданные для проведения тестирований на проникновение, позволяют автоматизировать большинство рутинных действий: от подготовки фишинговой кампании до разведки сети, повышения привилегий в системе и доставки итоговой программы (например, работающей с банкоматом) до конечной цели (банкомата). На то, что подобный сценарий развития событий вполне реален, указывают популяризация и романтизация образа компьютерных преступников некоторыми СМИ, а также фиксация появления большого количества «курсов для хакеров» на различных общедоступных интернет-форумах, позиционирующих себя как «Darknet-площадки», а также увеличение активности в тематических Telegram-каналах, где предлагаются различные услуги по обучению взлому и «сотрудничество» с целью заработка на создании ботнет-сетей, в том числе из устройств, принадлежащих кредитным организациям.

Последние имеющиеся у ФинЦЕРТ данные позволяют выдвинуть предположение о том, что в будущем крупные группы злоумышленников, пострадавшие от операций правоохранительных органов, реструктуризируются и продолжат свою деятельность, вероятно используя при этом новые инструменты проникновения, находящиеся на данный момент в разработке.

Факторы успешности целевых атак

Анализируя инциденты в сфере информационной безопасности кредитно-финансовых организаций, Банк России ведет работу по разработке системы стандартов и нормативно-правовых документов, соблюдение которых должно минимизировать ущерб от действий злоумышленников как банков, так и их клиентов. При этом пакет документов, который обязывает банки вести антифрод-мониторинг, был принят только в середине 2018 г., поэтому до настоящего момента динамика количества и объема атак снижалась относительно умеренными темпами.

По данным ФинЦЕРТ, в отчетный период было выявлено восемь основных причин успешности целевых атак, влияние которых в дальнейшем будет снижаться при условии соблюдения финансовыми организациями требований законодательства и регулятора:

1. Человеческий фактор: недостаточная грамотность сотрудников, открывающих подозрительные письма, пришедшие извне. *Согласно подпункту 2.12.1 Положения Банка России № 382-П «Оператор по переводу*

денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают повышение осведомленности работников в области обеспечения защиты информации:

– по порядку применения организационных мер защиты информации;

– по порядку использования технических средств защиты информации.».

Недостаточная грамотность сотрудников, открывающих подозрительные письма, указывает на недостаточную осведомленность работников кредитной организации (далее – КО) в области обеспечения защиты информации. Подобные вещи должны быть регламентированы во внутренних документах КО.

2. Отсутствие установленных актуальных обновлений на основные продукты, как правило, используемые в кредитных организациях: Microsoft Office, Microsoft Windows.

3. Неустановка обновлений (патчей) позволяет атакующим воспользоваться давно закрытыми уязвимостями программного обеспечения. В таблице 1 приведены основные используемые атакующими уязвимости, которые приводили к успешному исходу атаки.

4. Использование слабых паролей (либо хранение паролей в открытом виде в доступных атакующему местах) для критических элементов инфраструктуры (контроллеры домена, сервера, поддерживающие критические бизнес-процессы).

Такие нарушения, как использование слабых паролей (либо хранение паролей в открытом виде в доступных атакующему местах) для критических элементов инфраструктуры (контроллеры домена, сервера, поддерживающие критические бизнес-процессы), также должны быть регламентированы во внутренних документах КО. Подобные недостатки указывают на нарушения подпункта 2.6.3 Положения Банка России № 382-П в части необеспечения аутентификации участников платежной системы при осуществлении переводов денежных средств, а также подпункта 2.5.3 Положения, согласно которому «Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают контроль со стороны службы информационной безопасности соответствия создаваемых (модернизируемых) объектов информационной инфраструктуры требованиям технических заданий».

5. Отсутствие сегментирования сети.

Требования к сегментированию сети регламентированы п. 2.1 Главы 2 Положения Банка России № 552-П (в рамках участка Платежной системы Банка России), а также в подпункте 7.4.5 СТО БР ИББС-1.0-2014 (следует учитывать, что не все кредитные организации присоединены к СТО БР).

6. Отсутствие или неправильная настройка систем управления событиями информационной безопасности, что позволяет атакующему скрытно долгое время находиться в сети.

7. Неправильная настройка межсетевого экранирования.

8. Устаревшие антивирусные базы или отсутствие антивирусного программного обеспечения вообще.

Наличие антивирусного программного обеспечения регламентировано п. 2.7 Положения Банка России № 382-П, Главой 7 Положения Банка Рос-

сии № 552-П, п. 7.5 Главы 7 СТО БР ИББС-1.0-2014 (следует учитывать, что не все КО присоединены к СТО БР).

Банк России намерен в будущем способствовать совершенствованию систем обеспечения информационной безопасности кредитных организаций. С этой целью регулятор будет проводить политику по обязательному применению государственного стандарта ГОСТ Р 57580.1-2017, который сформулирован на основе анализа опыта выявления и предотвращения атак на информационные системы кредитных организаций и их клиентов и описывает детальный набор мер и средств по защите информации.

Основные типы уязвимостей, использование которых приводило к успешной атаке

№	Уязвимость	Описание	Устранение	Комментарий
1	CVE-2015-1641	Некорректно сформированный RTF-документ Microsoft Office	Установка пакетов обновления MS Office	Используется в начальной фазе атаки в фишинговом письме, позволяет атакующему загрузить программное обеспечение и установить связь с командным сервером для проведения дальнейшей атаки. Использовалась группой Carbanak (Cobalt Strike)
2	CVE-2014-1812 CVE-2014-4113 CVE-2015-1701 CVE-2015-2363 CVE-2015-2426 CVE-2016-7255	Повышение привилегий в ОС семейства Windows	Установка кумулятивных обновлений Windows через Центр обновления Microsoft	Используется в фазе закрепления, перемещения по сети, разведки сети для получения доступа к интересующим объектам сети. Используется различным специализированным ПО, таким как Cobalt Strike, Metasploit, Empire
3	CVE-2017-11882 CVE-2018-0802	Нарушение данных в области памяти Microsoft Office и его компонентов, позволяющее выполнить произвольный код	Установка пакетов обновления MS Office	Используется в начальной фазе атаки в фишинговом письме, позволяет атакующему загрузить программное обеспечение и установить связь с командным сервером для проведения дальнейшей атаки. Использовалась группой Carbanak (Cobalt Strike)
4	CVE-2017-0199 CVE-2017-8570	Уязвимости, связанные с некорректной обработкой встраиваемых в документ Microsoft Office Word различных объектов (подгружаемых данных из других документов и т.д.)		

НЕЦЕЛЕВЫЕ (СПАМ-АТАКИ) НА ОРГАНИЗАЦИИ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ

Данный класс атак отличается низкой эффективностью, поскольку подобные письма хорошо отфильтровываются спам-фильтрами. В то же время некоторый процент писем все-таки достигает конечных получателей. Их типовое содержание – различные «выигрыши», фишинг либо заражение майнинговым ВПО.

Содержание писем является важным элементом социальной инженерии. Оно является осмысленным и побуждает получателя открыть вложение или перейти по предлагаемой ссылке, либо как минимум снижает его опасения по поводу рискованности таких действий.

Текст писем иногда меняется в соответствии с текущей ситуацией в сфере интересов получателя. Такое письмо может сообщать о новых нормах законодательства, предстоящих изменениях в правилах бухгалтерского учета, предлагать обновить программное обеспечение. Иногда содержание прямо основывается на последних новостях из определенной сферы.

Письма, направляемые сотрудникам организаций, могут отличаться от писем, направляемых обычным гражданам. В организации обычно пишут про «отчеты», просят проверить «платежные документы», произвести «сверку», посмотреть «резюме». Граждан информируют о выигранных призах, поступивших на их счет денежных средствах или, наоборот, о назначенных взысканиях.

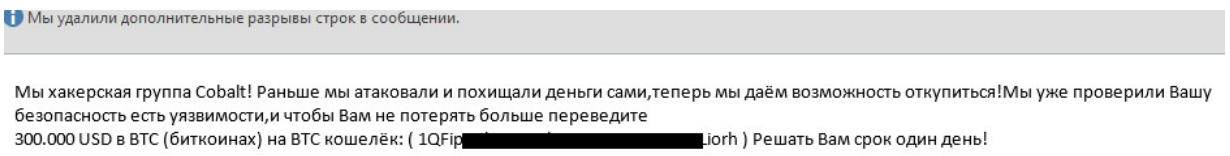
Относительно низкая доля пользователей, попадающихся на такие уловки, вынуждает злоумышленников рассылать письма одновременно в большое количество адресов. Так, например, ФинЦЕРТ наблюдает одновременные рассылки писем, предназначенных для внедрения ВПО на компьютеры сотрудников организаций кредитно-финансовой сферы, по спискам из нескольких тысяч адресатов. В итоге какая-то часть получателей все равно открывает вложения или ссылки из писем и, таким образом, исполняет вредоносный код. Этому способствует недостаточная личная «компьютерная гигиена» и, зачастую, низкий уровень обеспечения информационной безопасности в организации.

Согласно статистике ФинЦЕРТ, порядка 75% дошедших до адресата спам-писем – это различные виды майнеров, рассылаемых с использованием базы email-адресов, находящейся в свободном доступе в сети Интернет. Особого вреда компьютерной технике ВПО этого класса не наносит, однако может служить источником сильного раздражения пользователей из-за заметной траты вычислительных ресурсов и замедления производительности техники. Порядка 15% – письма различного фишингового содержания, также рассылаемые по доступным в сети Интернет базам email-адресов. Оставшиеся 10% – различного рода рекламные письма и письма-угрозы.

С мая по август 2018 г. специалисты ФинЦЕРТ отметили несколько волн мошеннических писем, направленных неизвестными лицами на официальные почтовые адреса финансовых организаций или через интернет-приемные финансовых организаций. В тексте писем их авторы называли себя членами группы Cobalt и требовали перечисления денежных средств в биткойнах, угрожая взломом систем, сетей банка и выводом сумм, значительно превышающих по размеру запрошенную. Пример письма показан на рисунке 15.

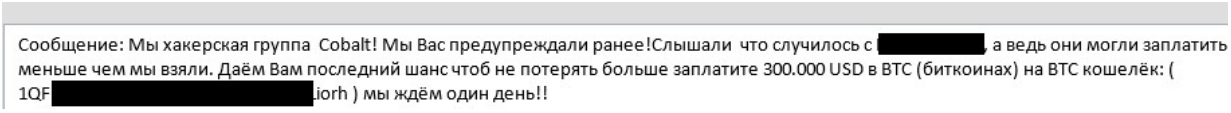
После публикации в ряде СМИ сообщений об успешной атаке на один из российских банков текстовка несколько изменилась (рис. 16).

Рисунок 15
Пример письма-угрозы якобы от имени Cobalt Strike


Мы удалили дополнительные разрывы строк в сообщении.

Мы хакерская группа Cobalt! Раньше мы атаковали и похищали деньги сами,теперь мы даём возможность откупиться!Мы уже проверили Вашу безопасность есть уязвимости,и чтобы Вам не потерять больше переведите
300.000 USD в BTC (биткоинах) на BTC кошелёк: (1QFip[redacted]iorh) Решать Вам срок один день!

Рисунок 16
Пример письма-угрозы якобы от имени Cobalt Strike


Сообщение: Мы хакерская группа Cobalt! Мы Вас предупреждали ранее!Слышали что случилось с [redacted], а ведь они могли заплатить меньше чем мы взяли. Даём Вам последний шанс чтоб не потерять больше заплатите 300.000 USD в BTC (биткоинах) на BTC кошелёк: (1QF[redacted]iorh) мы ждём один день!!

В ближайшем будущем предпосылок для существенных изменений наблюдаемой ФинЦЕРТ картины нет. Количество и уровень подготовки злоумышленников к подобным атакам, как мы полагаем, будут оставаться прежними. При этом возможно, что отдельные успешные крупные хищения в случае их освещения в СМИ в привязке к деятельности известных групп злоумышленников могут также сопровождаться несколькими волнами спам-рассылок мошеннических и вымогательских писем.

АТАКИ НА УСТРОЙСТВА САМООБСЛУЖИВАНИЯ

Как и в предыдущем отчетном периоде, различные атаки на устройства самообслуживания остаются в тренде. Основные типы атак, фиксируемых в России, – это blackbox (с физическим повреждением устройства) и проникновение на банкомат изнутри локальной сети банка для загрузки на него программного обеспечения, взаимодействующего с диспенсером и обеспечивающего выдачу наличных денежных средств.

Основное различие в фиксируемых blackbox-атаках и атаках изнутри сети кредитной организации – в способе доставки ВПО на банкомат: в первом случае носитель с этим ПО подключается непосредственно к банкомату, точнее к коммуникационным портам внутри банкомата (есть варианты с подключением промежуточного устройства – конвертера интерфейсов, подключаемого к ноутбуку злоумышленника и «в разрыв», то есть вместо какого-либо оборудования, входящего в состав банкомата), во втором случае появлению ВПО на банкомате предшествует компрометация инфраструктуры организации. Несмотря на это, часто бывает, что используется одно и то же ВПО, которого на рынке не так уж и много.

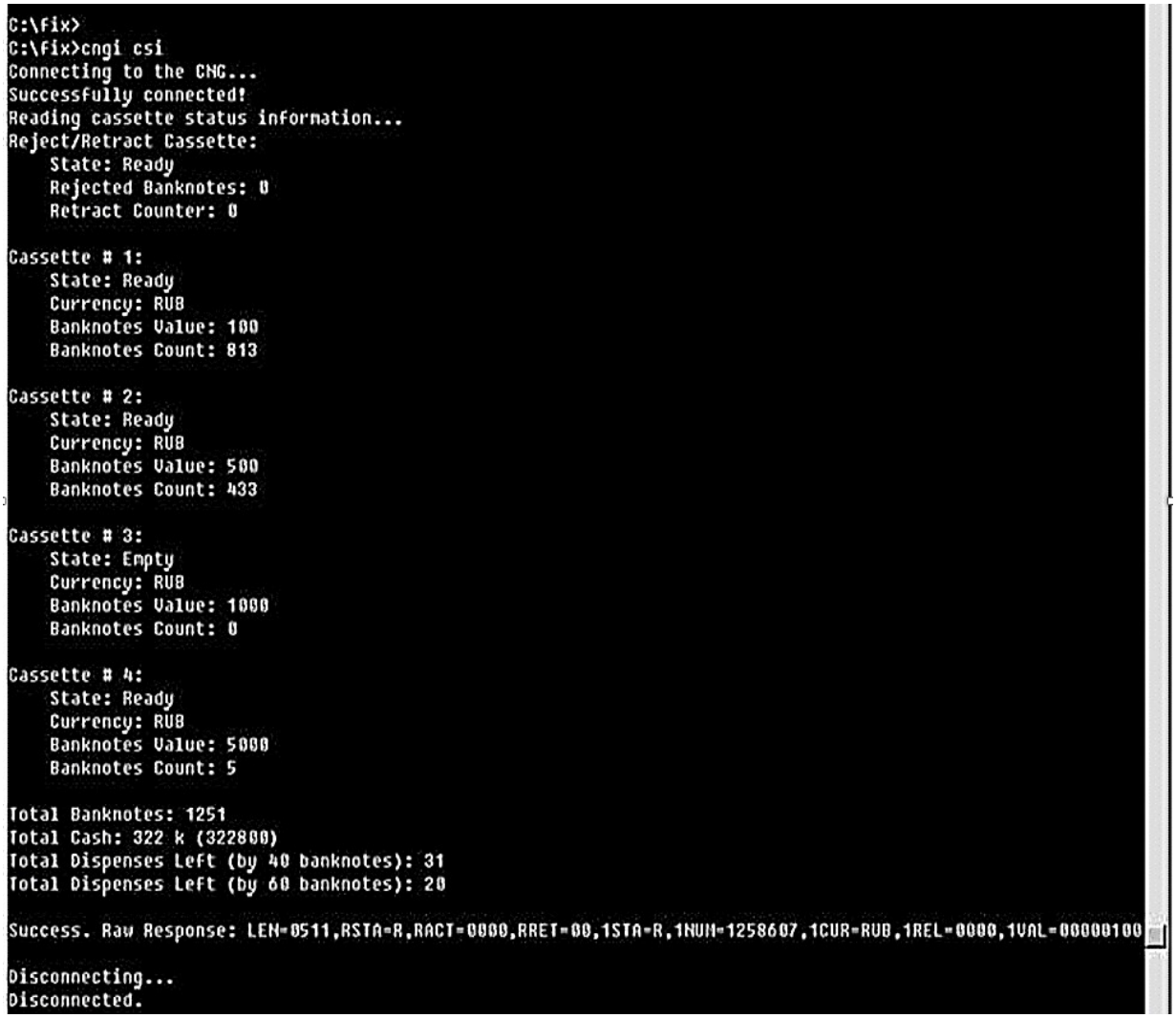
Число атак вида «скимминг» и «шимминг» неуклонно снижается, поскольку многие злоумышленники уже поняли, что копирование данных с магнитной полосы платежной карты – занятие бесперспективное ввиду обязательного выпуска чипованных карт, а копирование чипованных карт с последующей корректной обработкой клона карты банком-эмитентом в России бесполезно.

Не были зафиксированы случаи атак вида cash trapping – установка на банкомат специального устройства, удерживающего выдаваемую наличность для ее хищения после отхода от банкомата клиента, пытавшегося снять средства.

Стоит также отметить возросшее число попыток атак вида transaction reversal fraud (TRF) – воздействие на процесс обработки операции выдачи наличных денежных средств с тем, чтобы банкомат принял ошибочное решение о необходимости обратного зачисления денежных средств (reversal) на платежную карту, с которой производились снятие или перевод денежных средств (подробнее об этом см. подраздел «Мошенничество с отменой транзакций (TRF – Transaction Reversal Fraud)»).

Основные используемые программные средства при атаках – это программа cuinfo (название исполняемого файла может быть различным), обеспечивающая проверку наличия денежных средств в кассетах банкомата и выдающая необходимое количество купюр «дропу», находящемуся перед ним. Как правило, эта программа применяется при компрометации инфраструктуры кредитной организации. Внешний вид программы показан на рисунке 17.

Рисунок 17
Работа программы cuinfo



Хэш-суммы для определения указанной программы на банкоматах и ее промежуточного хранения в инфраструктуре организации ФинЦЕРТ рассылал в бюллетене FinCERT-20180823-01. В результате перепаковки программы или выхода новых версий хэш-сумма будет отличаться, поэтому необходимо применять меры по защите самого банкомата (о них ниже).

Другая распространенная программа, точнее программный комплекс – это Cutlet Maker, разработанный в среде Delphi. Комплекс состоит из трех программ: Cutlet Maker – обеспечивает выдачу дененжных средств (по одной или по 50 купюр), Stimulator – для проверки количества банкнот в диспенсере и их номинала и c0decalc – программа для генерации кодов, используемых Cutlet Maker.

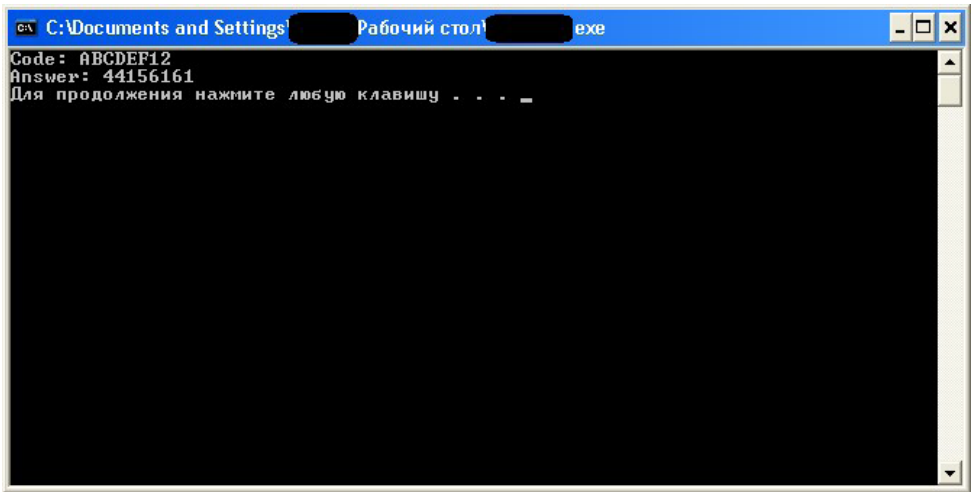
Рисунок 18
Интерфейс программы Cutlet Maker

Интересной особенностью Cutlet Maker является то, что его использование теоретически предполагает вовлечение в процесс хищения двух и более лиц. Код, снимающий блокировку с основных функциональных возможностей ВПО, генерируется отдельным приложением (c0decalc). Поэтому данный комплекс успешно используется при предоставлении услуги «взлом как сервис», которую ФинЦЕРТ описывал в отчете за 2017 год.

Интерфейс программ Stimulator и c0decalc показан на рисунках 19 и 20 соответственно.

Рисунок 19
Интерфейс программы Stimulator

Рисунок 20
Интерфейс программы c0decalc



В конце 2017 г. программа Cutlet Maker была выложена неизвестными лицами на открытые специализированные форумы сети Интернет и распространялась в Телеграм-чатах в полном объеме, включая c0decalc.

Данное обстоятельство, по мнению специалистов ФинЦЕРТ, указывает на эффективность программы ниже ожидаемого авторами программы минимума.

Для защиты от указанных программ в большинстве случаев достаточно составления «белого списка» разрешенных к запуску программ на банкоматах и использования надежного способа аутентификации (желательно 2FA) на управляющем сервере программы, контролирующей «белый список».

Атаки на устройства самообслуживания являются одним из самых популярных методов нелегального заработка среди киберпреступников, поэтому, скорее всего, их количество будет оставаться на сравнительно высоком уровне вплоть до момента повсеместного внедрения средств защиты, радикально усложняющих либо делающих принципиально невозможным несанкционированное снятие наличных денежных средств. Поэтому в новом отчетном периоде такая преступность сохранится, по нашему мнению, на прежнем уровне.

МОШЕННИЧЕСТВО С ОТМЕНОЙ ТРАНЗАКЦИЙ (TRF – TRANSACTION REVERSAL FRAUD)

Новый вид TRF-атак эксплуатирует ошибку в последовательности обработки запросов при выполнении отмены P2P-перевода

В 2018 г. было зафиксировано два основных способа мошенничества TRF: первый использует конструктивный недостаток некоторых моделей банкоматов, которые подготавливают наличность к выдаче, но держат ее за закрытой шторкой шаттера («пре-кэш»); действие второго направлено на нарушение логики работы процессингового программного обеспечения.

Первый вариант TRF: злоумышленник проводил «стандартный» съем наличных денежных средств, но не забирал карту из картоприемника. За время, пока банкомат не изымал карту, злоумышленник вскрывал шторку шаттера, повреждая механизм шторки, и забирал подготовленную наличность. При этом банкомат прекращал клиентское обслуживание («out of service») и считал, что денежные средства не выданы, в результате чего происходило восстановление баланса на счете.

Второй вариант TRF был направлен на эксплуатацию некорректности настроек некоторых процессинговых систем. Ошибка заключалась в последовательности обработки запросов банку-эквайреру и банку-эмитенту при выполнении операции возврата средств на карту отправителя в случае выполнения перевода от клиента к клиенту. Складывалась ситуация, когда на карту отправителя банк возвращал денежные средства, а от банка – эмитента карты получателя приходил отказ о возможности списания денежных средств, и деньги с получателя не списывались. В максимально короткое время после проведения такого рода операций происходило обналичивание обеих карт во избежание блокировки денежных средств.

ФинЦЕРТ предполагает, что в дальнейшем будет фиксироваться увеличение числа способов и попыток проведения TRF из-за их доступности даже для малоквалифицированных исполнителей, не обладающих достаточными знаниями в области информационных технологий и принципов работы платежных систем.

АТАКИ НА КЛИЕНТОВ КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

ФинЦЕРТ за отчетный период зафиксировал три основных вида атак на клиентов кредитных организаций. Конечная цель любой такой атаки – это получение доступа к управлению счетами организации путем установки на компьютере последней версии вредоносного программного обеспечения, обладающего функциональными возможностями из списка:

- предоставление удаленного доступа к зараженному компьютеру;
- кража учетных данных к системам ДБО;
- перехват и подмена реквизитов в платежных поручениях, направляемых через ДБО;
- создание подложных платежных поручений и отправка их в кредитную организацию.

ФинЦЕРТ наблюдал значительное количество атак, направленных на юридические лица, с использованием ВПО семейства Dimnie, оснащенного специальными модулями для работы с ДБО, а также ВПО семейства RTM. Так, за отчетный год подготовлены и направлены участникам информационного обмена оперативные бюллетени о 26 зафиксированных кампаниях распространения Dimnie и 10 кампаниях распространения RTM.

Рисунок 21
Изменения в файловой системе, инициированные дроппером RTM

Process Name	PID	Operation	Path
rtm_dropper.exe	176	WriteFile	C:\Documents and Settings\Admin\Local Settings\Temp\37.tmp
rtm_dropper.exe	176	WriteFile	C:\Documents and Settings\All Users\Application Data\bhmaglfj\gmmfgjim.hfd
rtm_dropper.exe	176	WriteFile	C:\Documents and Settings\All Users\Application Data\bhmaglfj\19be7fea7cc0
rtm_dropper.exe	176	WriteFile	C:\WINDOWS\Tasks\Windows Update 5dcb6e66.job
svchost.exe	1056	WriteFile	C:\WINDOWS\Tasks\Windows Update 5dcb6e66.job
rtm_dropper.exe	176	WriteFile	C:\WINDOWS\Tasks\Windows Update 5dcb6e66.job
rtm_dropper.exe	176	WriteFile	C:\WINDOWS\Tasks\Windows Update 7e71d810.job
rtm_dropper.exe	176	WriteFile	C:\WINDOWS\Tasks\Windows Update a534601b.job
rtm_dropper.exe	176	WriteFile	C:\WINDOWS\Tasks\Windows Update 5ac23e9d.job
svchost.exe	1056	WriteFile	C:\WINDOWS\Prefetch\RTM_DROPPER.EXE-10A234A1.pf
svchost.exe	1056	WriteFile	C:\WINDOWS\Tasks\Windows Update 5dcb6e66.job
svchost.exe	1056	WriteFile	C:\WINDOWS\SchedLgU.Txt
svchost.exe	1056	WriteFile	C:\WINDOWS\SchedLgU.Txt
svchost.exe	1056	WriteFile	C:\WINDOWS\SchedLgU.Txt
svchost.exe	1056	WriteFile	C:\WINDOWS\SchedLgU.Txt
svchost.exe	1056	WriteFile	C:\WINDOWS\Tasks\Windows Update 5ac23e9d.job
svchost.exe	1056	WriteFile	C:\WINDOWS\Tasks\Windows Update 7e71d810.job
svchost.exe	1056	WriteFile	C:\WINDOWS\Tasks\Windows Update a534601b.job
rundll32.exe	1764	WriteFile	C:\Documents and Settings\Admin\Local Settings\Temp\37.tmp
rundll32.exe	1764	SetRenameInformationFile	C:\Documents and Settings\Admin\Local Settings\Temp\37.tmp
rundll32.exe	1764	SetDispositionInformationFile	C:\Documents and Settings\Admin\Local Settings\Temp\dhponhlfalcdbfem
rundll32.exe	1764	WriteFile	C:\Documents and Settings\Admin\Рабочий стол\rtm_dropper.exe
rundll32.exe	1764	WriteFile	C:\Documents and Settings\Admin\Рабочий стол\rtm_dropper.exe
rundll32.exe	1764	WriteFile	C:\Documents and Settings\Admin\Рабочий стол\rtm_dropper.exe

Одной из особенностей ВПО семейств RTM и Dimnie является то, что для обращения к C&C-серверам часто используется альтернативная система доменных имен верхнего уровня Namecoin при помощи доменов «.bit». Такие домены не входят в официальный список организации ICANN и считаются abuse-устойчивыми (только владелец домена может изменить IP-адрес, на который он указывает, или прекратить его работу).

Распространение ВПО в основном происходит через рассылки фишинговых электронных писем. Основная масса файлов электронных документов-«приманок», используемых во вредоносной кампании RTM, имеют названия, характерные для бухгалтерской деятельности: «Отчет

для налоговой», «Окончательный счет на 01.01» и так далее. Иногда авторы писем используют отсылки к вновь принятому или вступившему в силу законодательству, причем делают это достаточно оперативно.

Компрометация порталов, имеющих массовую аудиторию

В течение года ФинЦЕРТ неоднократно фиксировал атаки типа watering hole, осуществлявшиеся через скомпрометированные порталы популярных средств массовой информации. При проведении такого вида атаки происходит скрытный взлом легального ресурса и, например, модификация системных файлов или отдельных страниц веб-сайта для размещения вредоносного кода. В результате этого при посещении ресурса пользователем браузер незаметно для него загружает и исполняет этот вредоносный код.

В последней зафиксированной атаке watering hole использовались уязвимости 2018 г. в Internet Explorer и ОС семейства Windows. Основной программный модуль Buhtrap, используемый при атаках данного вида, дает атакующему практически полный контроль над инфицированным компьютером. Таким образом в операционную систему пользователя может быть доставлено ВПО любого назначения. Разумеется, этим способом пользуются и злоумышленники, совершающие хищения со счетов клиентов кредитно-финансовых организаций.

В 2018 г. ФинЦЕРТ наблюдал четыре случая распространения ВПО Buhtrap, направленного на клиентов кредитных организаций (юридических лиц) через зараженные сайты популярных СМИ и отраслевых порталов, посещаемых банковскими работниками и бухгалтерами. По всем случаям ФинЦЕРТ осуществлял взаимодействие с владельцами ресурсов и предпринимал меры к блокировке доменов, на которых находился подгружаемый контент.

ФинЦЕРТ предполагает, что количество атак на юридические лица будет и далее возрастать. Защищенность кредитно-финансовых организаций улучшается высокими темпами, в том числе вследствие усилий ФинЦЕРТ, а также стандартизации и методологической работы в области информационной безопасности, проводимой Банком России. В то же время защищенность юридических лиц, не обязанных строго следовать требованиям регулятора, предъявляемым к организациям кредитно-финансовой сферы, зависит исключительно от степени интереса собственников бизнеса к защите информационных активов и возможностей ее обеспечить.

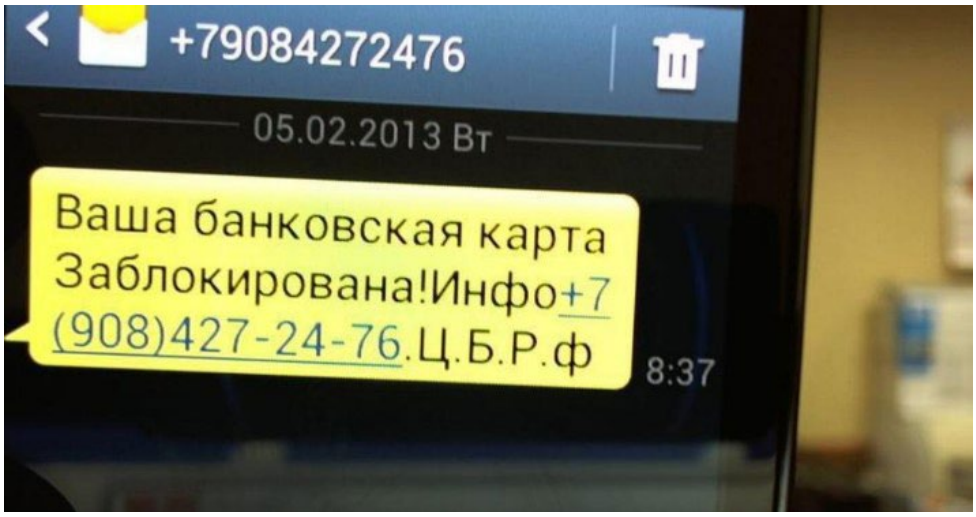
АТАКИ НА КЛИЕНТОВ – ФИЗИЧЕСКИХ ЛИЦ

Средствами физических лиц мошенники завладевают разными путями, но все они используют одну и ту же уязвимость – человеческий фактор. Беспечность, любопытство, доверчивость или стремление сэкономить – основные черты, которые используют злоумышленники для того, чтобы получить доступ к платежным реквизитам граждан или побудить в юридическом смысле добровольно расстаться с деньгами.

В целом атаки на физических лиц можно разделить на три вида в зависимости от категории жертв и наиболее эффективного способа коммуникации с ними. Так, в отношении наименее защищенных слоев населения,

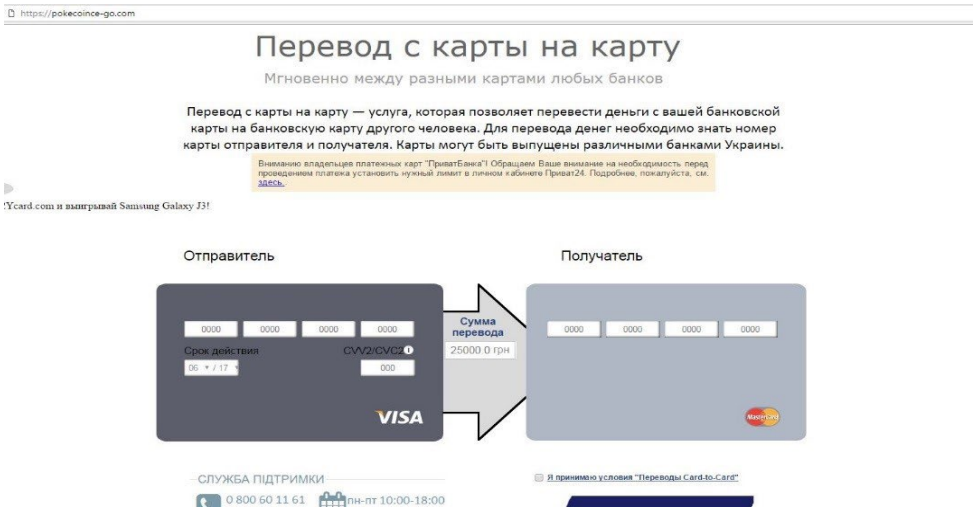
для которых характерен низкий уровень финансовой и киберграмотности (пенсионеры, лица с особыми потребностями, жители удаленных от федерального центра регионов и небольших городов), по-прежнему эффективны телефонные звонки и СМС с текстом наподобие «ваша карта заблокирована». Завладев вниманием жертвы и преодолев порог недоверия, злоумышленник побуждает ее сообщить платежные реквизиты или совершить перевод самостоятельно.

Рисунок 22
Блокировка» карты



Для экономически активной части населения, пользующейся Интернетом, актуальны другие способы вхождения в контакт. В первую очередь это спам-рассылки писем, содержание которых рассчитано на разные категории получателей. Это сообщения о скидках, получении компенсаций, предложения о знакомстве и другие заманчивые предложения, содержащие вредоносные файлы или ссылки на фишинговые сайты, которые сами по себе также являются способом коммуникации мошенников с жертвами. Получив такое письмо, человек открывает файл или переходит по ссыл-

Рисунок 23
Мошеннический ресурс по P2P-платежу



ке, в результате чего происходит заражение устройства и компрометация платежных данных его владельца.

Владельцы смартфонов также часто становятся жертвами злоумышленников – благодаря широкому распространению мобильных устройств под управлением ОС Android. Как правило, для получения доступа к их счетам преступники используют ВПО, работающее с системами СМС-банкинга или создающее поддельные окна приложений онлайн-банкинга. Такое ВПО часто характеризуется высокой степенью схожести в различных отдельных случаях, так как большинство «удачных решений» в коде злоумышленники используют повторно в новых версиях своих приложений или продают их на соответствующих интернет-порталах, включая Darknet.

Взлом аккаунтов в соцсетях

Последнее время набирает обороты взлом аккаунтов в соцсетях с целью рассылки по списку контактов их владельцев просьб о материальной помощи от их имени. Таким образом, наименее квалифицированными преступниками монетизируется наиболее дешевый «материал», возникающий как результат работы индустрии компьютерной преступности. Доступы к аккаунтам в социальных сетях продаются на теневых ресурсах оптом. Единица измерения этого товара – тысяча, а цены – от нескольких долларов за единицу (то есть за тысячу). Реквизиты доступа попадают в распоряжение взломщиков в процессе эксплуатации обширных бот-сетей. Из непригодных к чему-либо другому ботов – зараженных компьютеров «выжимают» хотя бы доступы к каким-либо сетевым ресурсам, которые потом продают. И это доступы не только к социальным сетям, но и к электронной почте, файловым хранилищам, веб-серверам. Монетизацией такого «материала» занимаются скупающие его преступники, зачастую начинающие, которые не нашли себе другой криминальной профессии. В то же время нужно ожидать, что по мере снижения доходов

от хищений компьютерам и аккаунтам простых обывателей преступность будет уделять все больше внимания, изыскивая любые новые возможности извлечения дохода, даже если для этого потребуется тщательный поиск и анализ компрометирующей информации, перехват переписки, шантаж, угрозы, вымогательство, продвинутые схемы мошенничества.

Каких-либо значимых субъективных предпосылок для снижения уровня атак данного вида ФинЦЕРТ не видит. В то же время практическое применение новых положений законодательства, направленных на недопущение неавторизованных переводов денежных средств, может сыграть решающую роль в значительном снижении количества атак на физических лиц.

ВЫВОДЫ И ПРОГНОЗЫ

Уровень защищенности организаций кредитно-финансовой сферы и их клиентов растет достаточно быстро, что не в последнюю очередь может быть результатом улучшения взаимодействия участников информационного обмена ФинЦЕРТ, а также стандартизации и методологической работы в области информационной безопасности, проводимой Банком России.

При этом защищенность некредитных финансовых организаций, которые на сегодняшний день не обязаны строго следовать требованиям регулятора, зависит исключительно от степени интереса собственников бизнеса к защите информационных активов и осознания необходимости обеспечения информационной безопасности в целом.

Можно предположить, что в обозримом будущем крупные группы злоумышленников, пострадавшие от операций правоохранительных органов, реструктуризируются и продолжат свою деятельность, используя, вероятно, новые инструменты проникновения, которые на сегодняшний день только разрабатываются.

По мнению ФинЦЕРТ, общий тренд снижения количества успешных крупных хищений у кредитных организаций сохранится. При этом число хищений у клиентов банков (юридических лиц и индивидуальных предпринимателей) может возрасти. Одна из возможных причин – утечка в Интернет исходного программного кода ВПО, используемого для таких хищений.

Количество атак на устройства самообслуживания будет оставаться на сравнительно высоком уровне до момента повсеместного внедрения средств и технологий защиты, которые радикально усложнят или сделают невозможным несанкционированное снятие наличных денежных средств.

Широкое освещение в СМИ атак группировок типа Cobalt Group может сопровождаться несколькими волнами спам-рассылок мошеннических и вымогательских писем более мелких мошеннических групп, пытающихся воспользоваться ситуацией и, мимикрировав под известные преступные группы, тем самым отвести от себя внимание.