Банк России

ОСНОВНЫЕ ТИПЫ КОМПЬЮТЕРНЫХ АТАК В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ В 2019–2020 ГОДАХ

Москва
2021

СОДЕРЖАНИЕ

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

Фото на обложке: Shutterstock/FOTODOM

107016, Москва, ул. Неглинная, 12

Официальный сайт Банка России: *www.cbr.ru*

СПИСОК СОКРАЩЕНИЙ

АС «Фид-АнтиФрод»	Автоматизированная система «Фид-АнтиФрод»
АСОИ ФинЦЕРТ	Автоматизированная система обработки инцидентов
Атака	В данном отчете за единичную атаку принимается вредоносная кампания в целом. Например, массовая атака, в рамках которой произошло несколько случаев заражения одним видом ВПО, рассматривается как одна уникальная
ВПО	Вредоносное программное обеспечение
ДБО	Дистанционное банковское обслуживание
Комплекс БР ИББС	Комплекс документов Банка России по стандартизации обеспечения информационной безопасности организаций банковской системы Российской Федерации, описывающий единый подход к построению системы обеспечения информационной безопасности организаций банковской сферы с учетом требований российского законодательства
Методы атаки	Совокупность приемов, которые использовались злоумышленниками для достижения цели
Мобильные устройства	Абонентские устройства мобильной связи, мобильные телефоны, смартфоны, коммуникаторы и другие устройства, используемые клиентами кредитных организаций при осуществлении переводов денежных средств
Операция без согласия клиента	Операции по переводу денежных средств, соответствующие утвержденным приказом Банка России от 27.09.2018 № ОД-2525 признакам осуществления перевода денежных средств без согласия клиента
Положение Банка России № 242-П	Положение Банка России от 16.12.2003 № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах»
Положение Банка России № 382-П	Положение Банка России от 09.06.2012 № 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» (утратило силу в связи с изданием Положения Банка России от 09.01.2019 № 672-П «О требованиях к защите информации в платежной системе Банка России»)
Положение Банка России № 684-П	Положение Банка России от 17.04.2019 № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»

Программа-шифровальщик (англ. ransomware)	Вредоносная компьютерная программа, осуществляющая скрытное шифрование компьютерной информации пользователя с последующим вымогательством денежных средств за расшифровку
Спуфинг	Подмена в электронном почтовом сообщении видимого адреса отправителя для обмана получателя
Указание Банка России № 5039-У	Указание Банка России от 25.12.2018 № 5039-У «О формах и порядке направления операторами по переводу денежных средств уведомлений о приостановлении зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств, о невозможности приостановления зачисления денежных средств на банковский счет получателя средств или приостановления увеличения остатка электронных денежных средств получателя средств»
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 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Фишинг	Вид мошенничества в сети Интернет, целью которого является получение каких-либо конфиденциальных данных пользователей
Форма отчетности 0403203	Форма отчетности 0403203 «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств», установленная Указанием Банка России от 09.06.2012 № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств»
Форма отчетности 0409258	Форма отчетности 0409258 «Сведения о несанкционированных операциях, совершенных с использованием платежных карт», установленная Указанием Банка России от 24.11.2016 № 4212-У «О перечне, формах и порядке составления и представления форм отчетности кредитных организаций в Центральный банк Российской Федерации»
Целевая атака	Атака, про которую достоверно установлено, что она направлена на организации кредитно-финансовой сферы. При этом атака может быть как массовой, направленной на многие организации сразу, так и индивидуальной, направленной на одну организацию
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)
Spear-phishing	Целевой фишинг с использованием приемов социальной инженерии или какой-либо заранее известной атакующему информации о цели

ОБРАЩЕНИЕ ЗАМЕСТИТЕЛЯ ПРЕДСЕДАТЕЛЯ БАНКА РОССИИ Г.А. ЗУБАРЕВА

Уважаемые коллеги!

Ландшафт киберугроз 2020 года практически целиком определяла пандемия COVID-19. Большинство организаций, в том числе в кредитно-финансовой сфере, в этот период переориентировались на работу в дистанционном режиме, что не только позволило обеспечивать потребности граждан, но и перестроило фокус внимания злоумышленников. По мере обнаружения новых угроз необходимо отслеживать и анализировать их динамику, учитывая ее при организации работы и корректируя подходы к обеспечению информационной безопасности. Чем длительнее анализируемый промежуток времени, тем эта работа эффективнее, поэтому мы приняли решение перенести публикацию обзора основных типов атак и включить в него сразу два периода – 2019 и 2020 годы.

Анализ представленной в обзоре информации позволит организациям финансового сектора понимать, в какой среде им придется развиваться, разрабатывать и выводить на рынок новые продукты и услуги в ближайшем будущем. Информационная безопасность традиционно следовала за бизнесом, но это опасная позиция, которая приводит к возникновению предпосылок реализации угроз. Эти риски необходимо минимизировать еще на стадии проектирования элементов информационной инфраструктуры.

Банк России как высокотехнологичный регулятор всемерно поддерживает развитие финансовых технологий. Например, в связи с задачей обеспечения безопасной реализации удаленного предоставления финансовых услуг одним из самых актуальных направлений мы сегодня видим выстраивание единой доверенной среды. С учетом того, что рынок будет неизбежно двигаться в сторону использования цифровых сервисов, основанных на новых технологиях – open API, биометрии, технологии распределенных реестров, наша с вами задача – заранее составить карту рисков на основе информации о той среде, в которой придется оперировать вашим организациям.

Банк России разрабатывает нормы, соблюдение которых обеспечивает учет и нивелирование поднадзорными организациями возможных рисков. Но финансовым организациям также необходимо работать с угрозами самостоятельно и на упреждение. Информация, представленная в обзоре, характеризует условия, в которых будут реализовываться инициативы по цифровизации бизнеса ваших организаций, и те риски, которые необходимо учитывать при реализации этих инициатив.

Рассчитываем, что наряду с самостоятельной работой в этом вам также поможет участие в киберучениях, которые проводятся с конца 2020 года. Данные, получаемые по каналам информационного обмена, используются при составлении сценариев, в ходе которых в режиме стресс-тестирования проверяется готовность подразделений информационной безопасности и информационных технологий поднадзорных организаций выявить и локализовать новые и актуальные угрозы. Иными словами, оценивается эффективность практического соблюдения нормативных требований организациями финансовой сферы в условиях реализации угроз, информация о которых регулярно доводится в оперативных бюллетенях ФинЦЕРТ.

Уверен, что обзор будет полезен в работе по обеспечению операционной надежности и киберустойчивости ваших организаций. Эти составляющие являются необходимым условием развития и обеспечения стабильности финансового рынка, национальной платежной системы, укрепления банковской системы и развития экономики Российской Федерации.

ВВЕДЕНИЕ

В настоящем обзоре приводятся сведения об основных типах атак в кредитно-финансовой сфере, зафиксированных ФинЦЕРТ в 2019 и 2020 годах. Если в 2019 году Банк России наблюдал продолжение трансформации угроз в кредитно-финансовой сфере, то в 2020 году ландшафт угроз определяла эпидемия новой коронавирусной инфекции. В силу своей неожиданности она фактически стала «черным лебедем», кардинально и негативно изменившим все стороны социальной и экономической жизни, включая обеспечение информационной безопасности финансовых организаций и их клиентов. Основную роль сыграл перевод деловой, социальной, а также повседневной бытовой экономической активности в дистанционный формат.

И если финансовые организации были относительно неплохо подготовлены к негативным изменениям, то их клиенты – как физические, так и юридические лица – столкнулись с таким ростом числа атак и их разнообразием впервые. Атаки с использованием методов социальной инженерии на клиентов банков – держателей банковских карт и счетов – показали значительный количественный рост и прогресс в качестве воздействия. Добавление в схемы введения в заблуждение полученных из различных источников персональных данных, а также применение более узконаправленных, кастомизированных приемов социальной инженерии в рассматриваемый период многократно повысило эффективность и доходность, казалось бы, уже давно известного, так называемого телефонного мошенничества.

Спрос на конфиденциальные данные клиентов, используемые для преодоления порога недоверия клиентов банков, привел к резкому увеличению рынка незаконно полученных баз данных финансовых организаций и услуг по «пробиву» счетов клиентов. Весь рассматриваемый период был отмечен резонансными утечками как из финансовых, так и из других организаций, не относящихся к числу поднадзорных Банку России.

Другой важной тенденцией года стало продолжение многолетнего снижения количества наиболее опасных целевых атак на информационную инфраструктуру финансовых организаций, вплоть до их почти полного прекращения. Массовые рассылки вредоносных программ типа Cobalt Strike и Silence, привлекавших особое внимание индустрии информационной безопасности в прошлые годы, по спискам адресов сотрудников почти прекратились. Редкие результативные взломы привели к весьма незначительному по сравнению с прошлыми годами ущербу. Также почти полностью прекратились атаки на устройства банковского самообслуживания. При этом имеющиеся в распоряжении Банка России данные позволяют сделать предположение о появлении как минимум одной группы атакующих, сосредоточившихся на квалифицированном взломе финансовых мобильных приложений.

Клиенты финансовых организаций – юридические лица и индивидуальные предприниматели, относящиеся к категории малого и среднего бизнеса, – подвергаются риску. Хакерские группы, которые за ними охотятся, действуют целенаправленно, с возрастающей настойчивостью и технической изобретательностью.

Любопытные изменения наблюдаются в части атак с использованием программ-шифровальщиков. Несмотря на эффектный, публично освещаемый уход из этого бизнеса операторов ряда хорошо известных программ, их общее количество по всему миру не уменьшилось. Однако именно от финансовых организаций стало поступать существенно меньше сообщений о выявлении шифровальщиков.

Об этих и других тенденциях мы рассказываем в данном обзоре. Информация из него предназначена для использования руководителями и специалистами служб информационной безопасности в целях планирования стратегий и отдельных мероприятий и для повышения осведомленности широкого круга сотрудников финансовых организаций и их клиентов об основных актуальных угрозах.

КОМПЬЮТЕРНЫЕ АТАКИ В 2019–2020 ГОДАХ

Основные результаты по данным АСОИ ФинЦЕРТ

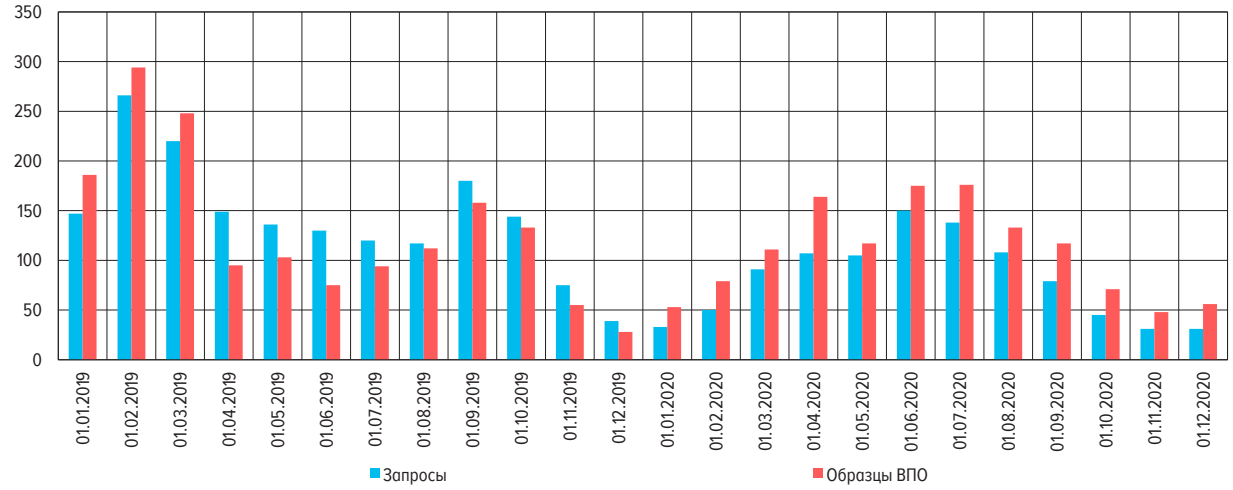
Банк России ведет информационный обмен с поднадзорными организациями через Автоматизированную систему обработки инцидентов (АСОИ ФинЦЕРТ). Массив информации, собранный за два года, позволяет провести детальный анализ по нескольким направлениям.

В 2020 году через АСОИ ФинЦЕРТ от участников информационного обмена в процессе информирования об указанных выше попытках компьютерных атак было получено 968 сообщений о фактах распространения ВПО, содержавших 1300 образцов ВПО.

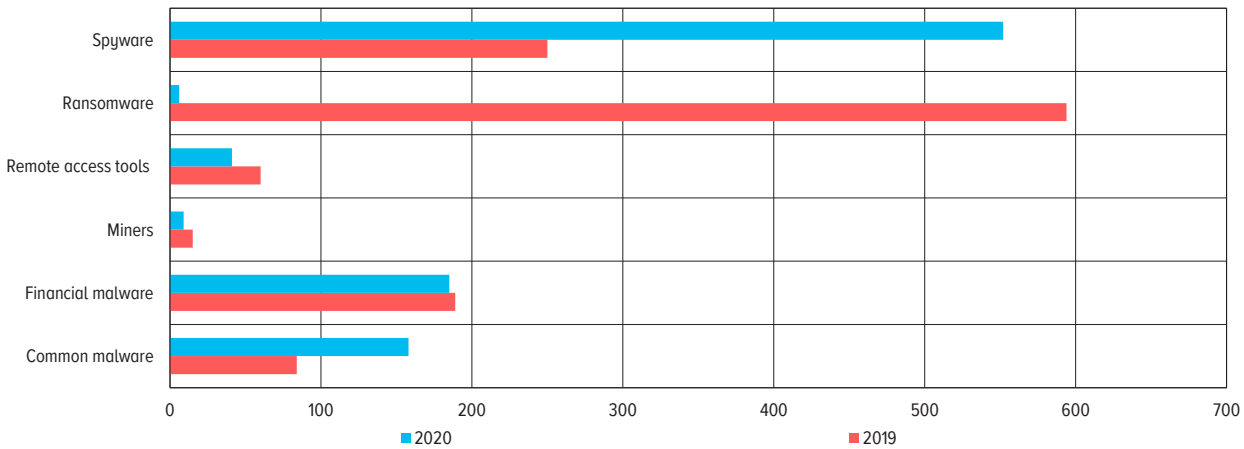
Годом ранее было зафиксировано 1723 обращения, содержавших 1581 образец ВПО. Большинство этих случаев – распространение различного ВПО с использованием электронной почты.

Сравнение структуры исследованного объема ВПО с данными 2019 года позволяет выделить несколько тенденций. Так, если в 2019 году программы-шифровальщики оставались

ПОСТУПИВШИЕ В 2019–2020 ГГ. ЗАПРОСЫ О ФАКТАХ РАСПРОСТРАНЕНИЯ ВПО И ИССЛЕДОВАННЫЕ ОБРАЗЦЫ (ЕДИНИЦ) *Рис. 1*



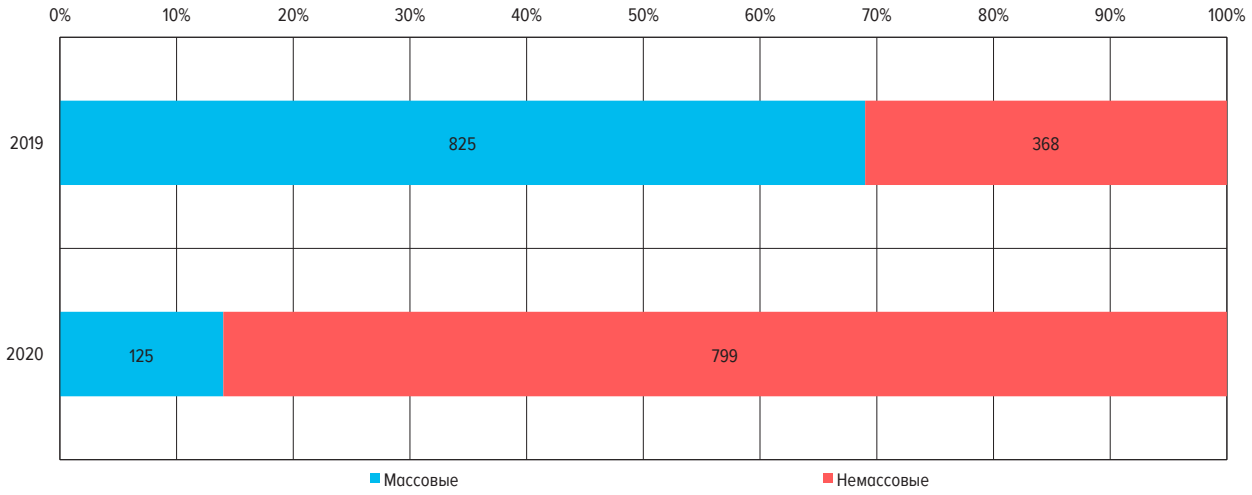
РАСПРЕДЕЛЕНИЕ ВПО ПО КЛАССАМ, 2019–2020 ГОДЫ (ЕДИНИЦ) *Рис. 2*



Примечание. Common malware – различное ВПО, financial malware – ВПО для атак на финансовые организации, miners – майнеры криптовалют, remote access tools – средства удаленного доступа, ransomware – программы-шифровальщики, spyware – шпионское ВПО.

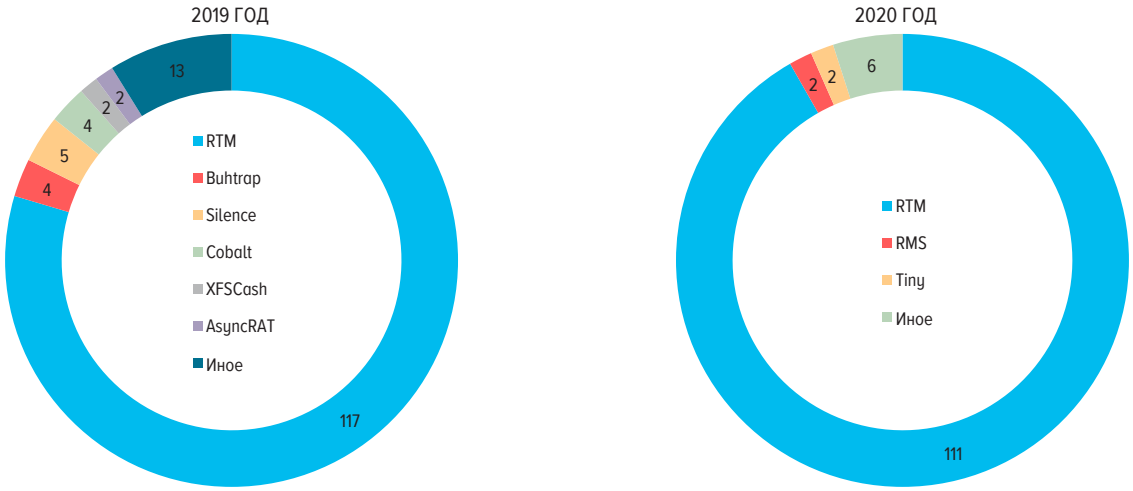
МАССОВОСТЬ РАССЫЛОК ВПО
(ЕДИНИЦ)

Рис. 3



КОЛИЧЕСТВО БЮЛЛЕТЕНЕЙ С РАСПРЕДЕЛЕНИЕМ ПО ТИПУ УГРОЗ
(ЕДИНИЦ)

Рис. 4



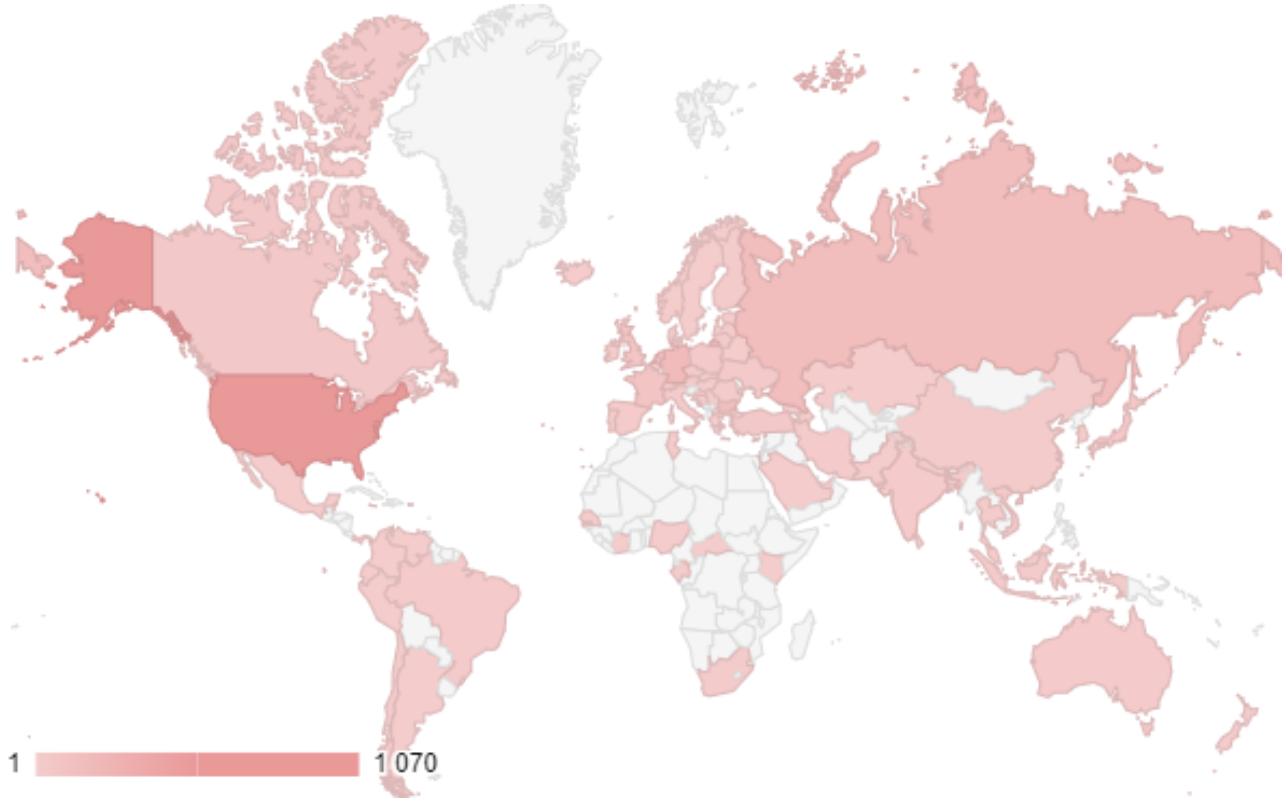
на первом месте (50%), а второе место занимало шпионское ПО (21%), то в 2020 году на первое место вышло шпионское ПО, доля которого выросла более чем в 2,5 раза, что позволило ему оказаться на первом месте по числу исследованных образцов (58%), тогда как второе место досталось финансовому ВПО (примерно 13%). О практически полном уходе в 2020 году программ-шифровальщиков рассказано в отдельной главе. ВПО для банкоматов выявлялось в единичных случаях.

По признаку количества адресатов одной атаки заметно возрастание атак немассовых. Так, в 2020 году только 15,6% атак были массовыми, в то время как в 2019 году их доля составляла 69%. Инициаторы атак перестраиваются в связи с постоянно возрастающим противодействием: в условиях развития корпоративных и отраслевых центров реагирования массовые атаки выявляются и пресекаются гораздо быстрее, часто становясь бесполезными.

По наиболее опасным компьютерным атакам ФинЦЕРТ в 2019–2020 годах продолжил практику выпуска оперативных бюллетеней, представляемых как в формате документа Adobe PDF, так и в машиночитаемых форматах. Каждый бюллетень содержит описание атаки, ее основные индикаторы компрометации и в отдельных случаях – рекомендации по предупреждению, пресечению и устранению последствий. Всего в 2019 году участникам информационного обмена

РАСПОЛОЖЕНИЕ ИНФРАСТРУКТУРЫ АТАК
(ЕДИНИЦ)

Рис. 5



США	1070
Германия	178
Россия	153
Болгария	152
Нидерланды	139
Франция	90
Великобритания	70
Канада	46
Япония	44
Турция	40
Украина	37
Сингапур	34
Вьетнам	30
Польша	29
Индия	25
Италия	24
Испания	24
Австралия	22
Иран	19
Бразилия	18
Чехия	18
Гонконг	15
Индонезия	14
Таиланд	13
Румыния	12
Китай	11
Южная Африка	10
Австрия	10

Латвия	10
Финляндия	10
Дания	9
Швейцария	8
Португалия	7
Чили	7
Литва	7
Казахстан	6
Швеция	6
Норвегия	6
ОАЭ	6
Аргентина	6
Словакия	5
Бельгия	5
Сейшелы	4
Южная Корея	4
Грузия	4
Ирландия	4
Габон	3
Эквадор	3
Сербия	3
Панама	3
Новая Зеландия	3
Колумбия	3
Хорватия	3
Перу	3
Кипр	2
Ямайка	2

Азербайджан	2
Мексика	2
Сенегал	2
Нигерия	2
Македония	2
Венгрия	2
Бангладеш	2
Саудовская Аравия	2
Беларусь	2
Исландия	2
Венесуэла	2
Малайзия	2
Шри-Ланка	1
Кот-д'Ивуар	1
Эстония	1
Пакистан	1
Голландия	1
Центрально-Африканская Республика	1
Пуэрто-Рико	1
Израиль	1
Тунис	1
Босния и Герцеговина	1
Белиз	1
Непал	1
Кения	1
Греция	1

было направлено 147 оперативных бюллетеней, в 2020 году – 121. Большинство бюллетеней в 2020 году было посвящено атакам группы RTM.

Расположение ресурсов в сети Интернет – серверов для рассылки электронных писем, серверов для распространения ВПО, управляющих серверов ВПО – показано на карте и в таблице (рис. 5). Наибольшее количество таких ресурсов размещалось, как и в предыдущие годы, вне территории Российской Федерации – преимущественно в странах, где традиционно находится большинство веб-серверов.

Атаки на информационную инфраструктуру организаций кредитно-финансовой сферы Российской Федерации

С момента создания ФинЦЕРТ предотвращение атак на инфраструктуру организаций кредитно-финансовой сферы является одной из важнейших задач в связи с их высокой опасностью для операционной деятельности и потенциально большим ущербом. Особое внимание всегда уделялось раннему выявлению атак злоумышленников, специализирующихся на проникновении в инфраструктуру финансовых организаций для получения доступа к системам, позволяющим осуществлять переводы денежных средств на контролируемые атакующими счета. Традиционными целями в предыдущие годы были программные средства клиентов Банка России для переводов денежных средств по корреспондентским счетам, средства управления процессингом платежных карт, системы управления устройствами банковского самообслуживания, различные платежные шлюзы, средства системы SWIFT. Наиболее известными инструментами для атак групп злоумышленников, благодаря которым они часто получали в экспертных кругах свои условные наименования, были вредоносные программы Buhtrap, Cobalt Strike, Silence и некоторые другие.

Как мы отметили в начале обзора, в 2019 году количество наиболее опасных целевых атак со стороны подобных групп на информационную инфраструктуру организаций кредитно-финансовой сферы продолжало снижаться. Причины снижения имеют как фундаментальный, так и субъективный характер. К первым относится постепенное, неуклонное улучшение состояния защищенности информационных инфраструктур финансовых организаций, достигаемое за счет совершенствования систем управления информационной безопасностью и расширения состава используемых средств защиты информации, а также повышения профессионального уровня сотрудников подразделений информационной безопасности и информационных технологий. Другая причина – значительное снижение эффективности массовых рассылок в условиях функционирования системы информационного обмена ФинЦЕРТ. О любой рассылке в течение короткого времени, необходимого для подготовки и направления оперативного бюллетеня, становится известно всем финансовым организациям. Атакующие не успевают закрепиться в инфраструктуре до принятия защитных мер, даже если первичное проникновение было успешным. В результате усилия и средства, затраченные на подготовку атаки и рассылку ВПО, оказываются потерянными. Субъективные причины – постепенное выбывание участников и партнеров преступных групп в результате действий правоохранительных органов разных стран, деанонимизация, объявление в национальный или международный розыск. Важно, что злоумышленники российского происхождения перестали рассматривать перемещение за границу как легкий способ избежать ответственности. Многочисленные случаи задержания российских хакеров по всему миру по запросам иностранных государств делают любой выезд за границу крайне рискованным. На родине их активно ищут и находят российские правоохранительные органы, накопившие значительный объем оперативной информации и следственно-судебной практики. К субъективным причинам отказа от атак на финансовые организации может быть отнесено и развитие других прибыльных и пока более безопасных направлений криминального бизнеса: социальной инженерии, скрытого майнинга криптовалют, атак на владельцев криптовалют и объекты криптовалютной индустрии.

Как следует из указанного выше, в 2019 году ФинЦЕРТ получил от участников информационного обмена сравнительно небольшое количество сообщений о рассылках по электронным адресам финансовых организаций наиболее опасного вредоносного программного обеспечения. Атаки с использованием ВПО, известного как Silence, были зафиксированы минимум три раза – в январе, феврале и июне. Причем именно январская рассылка стала самой массовой. По сообщениям ряда экспертных организаций сферы информационной безопасности, число получателей данной рассылки составило около 80 тысяч.

Атаки с использованием программного обеспечения для тестирования на проникновение Cobalt Strike, официально выпускаемого компанией Strategic Cyber и активно используемого в криминальных целях по всему миру, были зафиксированы минимум четыре раза – в апреле, мае, июле и сентябре. Причем апрельская рассылка была точечной и выявлена только в единичном случае, майская ориентирована больше на банки из Казахстана и попала в российские организации, вероятно, случайно, зато июльская и сентябрьская были подготовлены на высоком техническом уровне и представляли реальную опасность для финансовых организаций.

Почти все эти атаки закончились без значимых результатов, с единичными успешными проникновениями в информационную инфраструктуру и сравнительно небольшим ущербом, что в итоге привело к завершению либо трансформации деятельности участников соответствующих групп. Последнее более вероятно, причем в виде переориентации на страны ближнего и дальнего зарубежья, из которых сообщения об атаках Cobalt Strike продолжают поступать и до настоящего времени. Необходимо отметить, что страна размещения используемой хакерами инфраструктуры и географический вектор атаки могут различаться.

Технология атак с использованием указанных видов ВПО на информационную инфраструктуру финансовых организаций в целом значимых изменений с 2017 года не претерпела. Первоначальное проникновение идет через фишинговые письма (spear-phishing), рассылаемые по списку электронных адресов сотрудников организаций. Часто письма направлялись якобы от имени каких-либо других финансовых организаций или органов государственной власти. ВПО обычно содержится во вложениях таких писем. Чуть реже используется вариант, когда файл предлагается загрузить с внешнего ресурса по ссылке из тела письма.

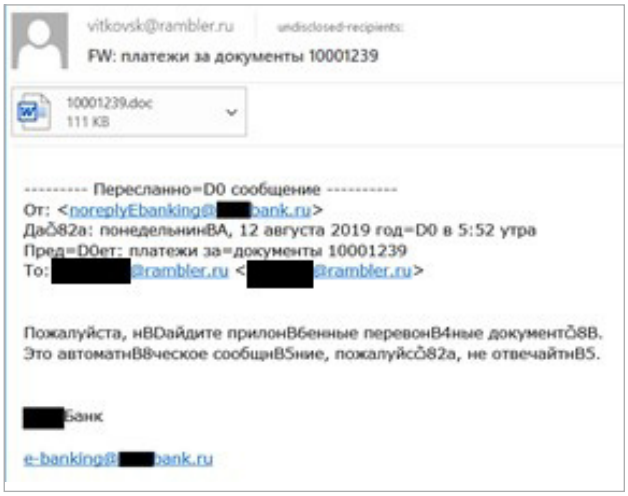
После открытия вложения или загруженного файла (чаще всего документа формата программного пакета Microsoft Office) происходят скрытая загрузка и запуск программного обеспечения, предоставляющего атакующим удаленный доступ к компьютеру. В абсолютном большинстве известных случаев для внедрения кода использовались уже известные уязвимости указанного программного пакета. Иными словами, успех атакующих обуславливался в числе прочего и использованием несвоевременно обновляемого и сохраняющего широко известные уязвимости программного обеспечения, установленного на рабочих компьютерах сотрудников организаций.

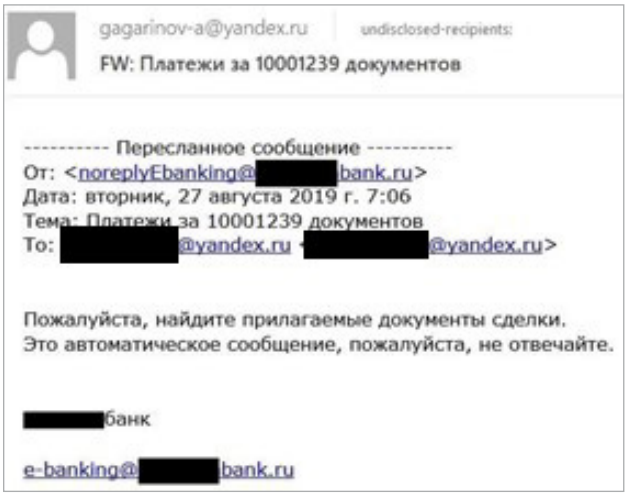
После проникновения в первый компьютер атакующие проводили изучение доступного сегмента локальной сети, выявляли другие представляющие интерес компьютеры и серверы, проникали и закреплялись в них, а затем приступали к подготовке хищения. В случае если у атакованной организации не было своего процессинга, но имелся платежный шлюз, атакующие пытались использовать его для передачи подложных платежных поручений либо поручений для изменения баланса платежных карт (при использовании процессинговых центров).

Еще раз отметим, что в 2019 году почти все эти традиционные схемы остались безрезультатными, за исключением единичных случаев с небольшим ущербом. И конечно, атаки непосредственно на инфраструктуру финансовых организаций не ограничивались только указанными вредоносными инструментами. В течение года ФинЦЕРТ получал информацию от участников обмена о выявлявшихся случаях целевых атак на финансовые организации с использованием иных, менее распространенных или не столь раскрученных семейств ВПО, преимущественно класса RAT (Remote Access Tool). В частности, выявлялись AsyncRAT, TeamBot (модифициро-

ванный Team Viewer) и некоторые неопознанные, предположительно приватные инструменты. Их количество именно в целевых атаках на финансовые организации, а не на случайно попавшие в рассылки, также осталось весьма незначительным на фоне прошлых лет.

При этом такие рассылки могли быть достаточно опасными, поскольку получателей умело вводили в заблуждение. Так, кампании по распространению ВПО AsyncRAT велись с использованием названий ряда поднадзорных организаций.





Во вложении такого письма находился документ, содержавший эксплойт уязвимости CVE-2017–11 882. В результате происходило обращение по указанному в теле сетевому адресу для загрузки полезной нагрузки – ВПО AsyncRAT, которое, помимо стандартного функционала средства для удаленного мониторинга и управления рабочим столом, также имеет встроенный кейлоггер. Первичное проникновение такого ВПО может иметь тяжелые последствия при развитии атаки по схеме, описанной выше.

В целом 2019–2020 годы оказались для финансовых организаций более безопасными с точки зрения целевых атак на инфраструктуру с использованием ВПО.

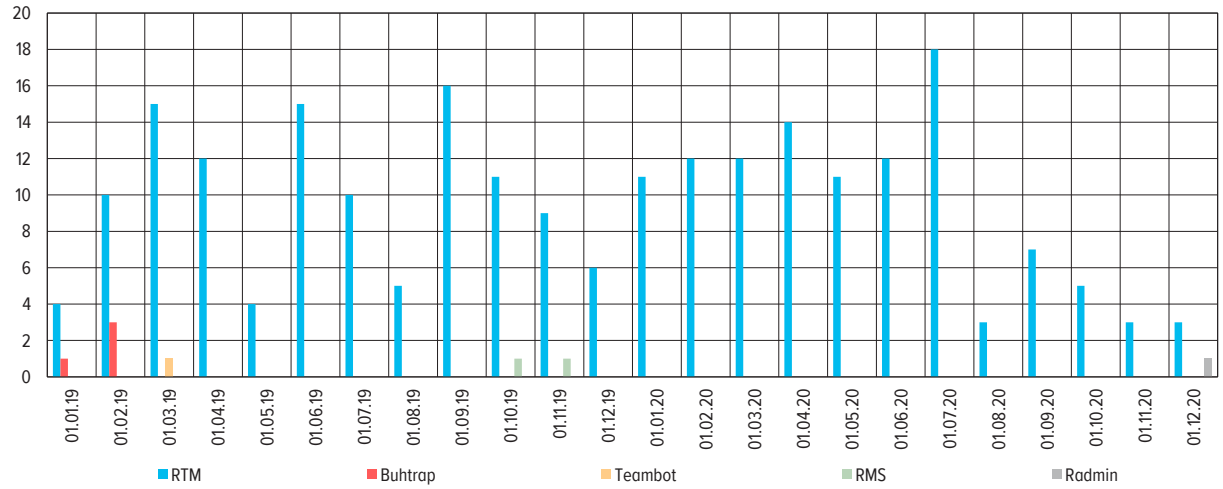
Атаки на информационную инфраструктуру клиентов организаций кредитно-финансовой сферы Российской Федерации

В 2019–2020 годах основной и наиболее активной угрозой для клиентов организаций кредитно-финансовой сферы, являющихся юридическими лицами и индивидуальными предпринимателями и использующими персональные компьютеры для доступа к системам дистанционного банковского обслуживания (ДБО), продолжала оставаться группа злоумышленников, хорошо известная под наименованием RTM (сокращение от самоназвания Remote Transaction Manager, обнаруженного в коде ВПО). За 2019–2020 годы ФинЦЕРТ получил информацию о 225 атаках данной группы. В среднем фиксировалось 2–3 атаки еженедельно, что указывало на очень высокую интенсивность работы группы.

Другие виды ВПО в целевых атаках на клиентов выявлялись в единичных количествах. Так, в январе и феврале 2019 года было четыре рассылки ВПО Buhtrap, ранее известного по атакам на программные средства АРМ КБР (Автоматизированное рабочее место клиента Банка России) ряда российских банков. А в октябре и ноябре 2020 года на фоне спада активности группы RTM было зафиксировано несколько рассылок ВПО, основным компонентом которого являлась утилита для удаленного доступа RMS. В декабре 2020 года был отмечен единичный случай рассылки ВПО, основным компонентом которого уже стала программа для удаленного доступа RAdmin. Вполне возможно, что инициатором этих атак была та же группа RTM, экс-

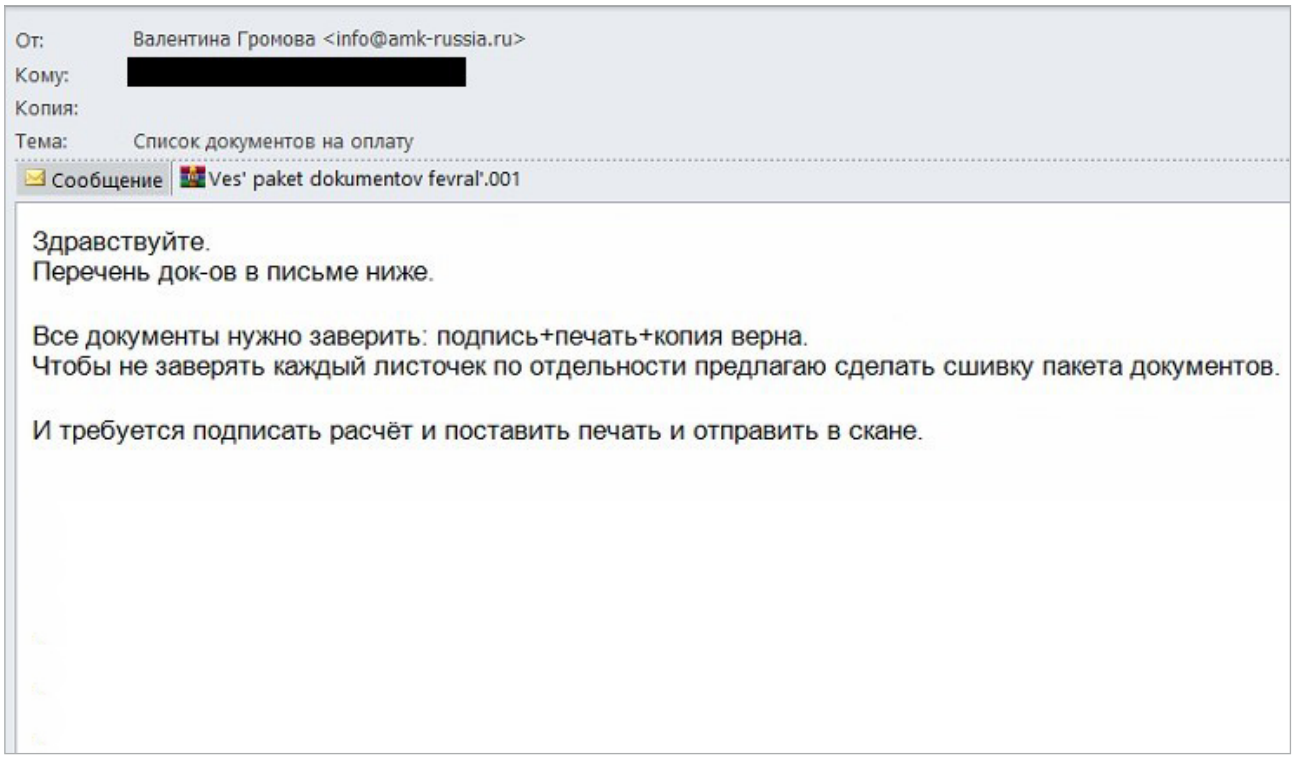
АТАКИ НА КЛИЕНТОВ ОРГАНИЗАЦИЙ ПО ТИПАМ ВПО
(ЕДИНИЦ)

Рис. 6



периментирующая с альтернативными инструментами. В марте 2019 года отмечена единичная рассылка по адресам клиентов финансовых организаций ВПО TeamBot, являющегося модифицированной версией популярной программы для удаленного администрирования компьютера TeamViewer. И все эти немногочисленные случаи только подчеркивали тотальное доминирование RTM.

Большая часть выявленных случаев атак RTM относится к фишинговым кампаниям, в которых к сообщениям электронной почты прикреплялся архив, содержавший файл с так называемой полезной нагрузкой.


От: Валентина Громова <info@amk-russia.ru>
Кому: [redacted]
Копия:
Тема: Список документов на оплату
Сообщение | Ves' paket dokumentov fevral'.001

Здравствуйте.
Перечень док-ов в письме ниже.

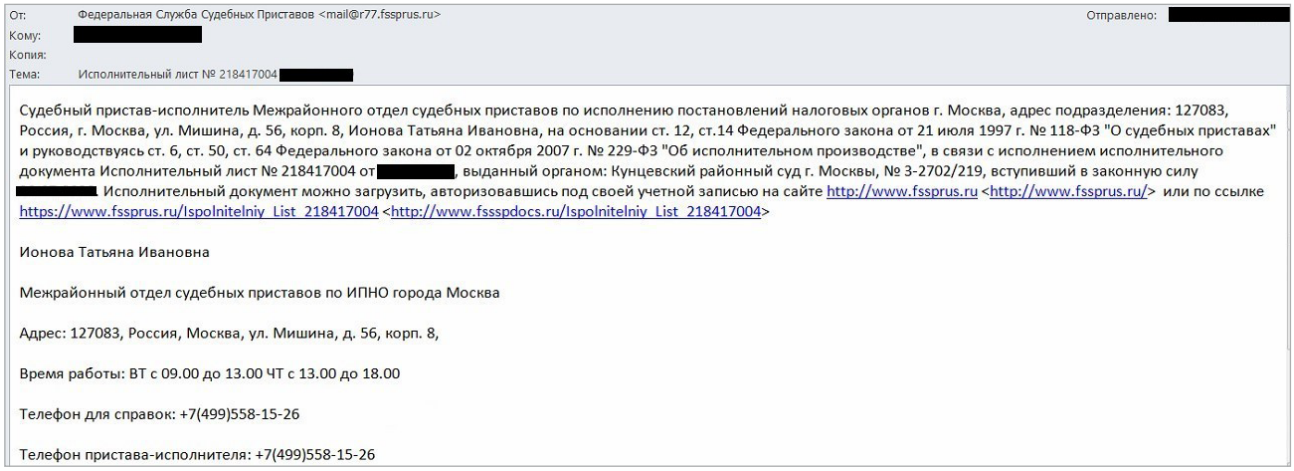
Все документы нужно заверить: подпись+печать+копия верна.
Чтобы не заверять каждый листочек по отдельности предлагаю сделать сшивку пакета документов.

И требуется подписать расчёт и поставить печать и отправить в скане.

Реже фишинговые кампании осуществлялись от имени конкретной организации, как, например, в случае с рассылкой от имени несуществующей «Профт Групп». И даже в таких случаях атакующими использовались подменные электронные почтовые адреса.


[redacted]er@proft.ru>
Профт Групп Россия · Запрос клиента: 0013709
Кому: [redacted]
Это сообщение было отправлено с важностью: Высокая.
Сообщение Запрос клиента 0013709.rtf (917 КБайт)
Пожалуйста, подтвердите наличие и укажите ваши лучшие цены.
С уважением,
Максим Янчевский
Центр опроса клиентов
Профт Групп Россия
г. Челябинск, Калининский р-н,
ул. Механическая д 115,
въезд с автодороги «Меридиан»
Тел: +7 (351) 211-59-55, +7 (951) 810-35-47
уведомление о конфиденциальности
Щелкните, чтобы скачать это письмо, подождите о том, чтобы обновить это.

В более сложно организованных вариантах рассылка фишинговых писем осуществлялась от имени одного из федеральных органов власти. Так, в рассылке от имени Федеральной службы судебных приставов (ФССП РФ) пользователю предлагалось загрузить файл по ссылке. Для этого атакующими был зарегистрирован домен, схожий по написанию с официальным доменом ФССП, – fssspdocs.ru.


От: Федеральная Служба Судебных Приставов <mail@r77.fssprus.ru> Отправлено: [redacted]
Кому: [redacted]
Копия:
Тема: Исполнительный лист № 218417004 [redacted]

Судебный пристав-исполнитель Межрайонного отдел судебных приставов по исполнению постановлений налоговых органов г. Москва, адрес подразделения: 127083, Россия, г. Москва, ул. Мишина, д. 56, корп. 8, Ионова Татьяна Ивановна, на основании ст. 12, ст.14 Федерального закона от 21 июля 1997 г. № 118-ФЗ "О судебных приставах" и руководствуясь ст. 6, ст. 50, ст. 64 Федерального закона от 02 октября 2007 г. № 229-ФЗ "Об исполнительном производстве", в связи с исполнением исполнительного документа Исполнительный лист № 218417004 от [redacted], выданный органом: Кунцевский районный суд г. Москвы, № 3-2702/219, вступивший в законную силу [redacted]. Исполнительный документ можно загрузить, авторизовавшись под своей учетной записью на сайте http://www.fssprus.ru <http://www.fssprus.ru/> или по ссылке https://www.fssprus.ru/Ispolnitelniy_List_218417004 <http://www.fssspdocs.ru/Ispolnitelniy_List_218417004>

Ионова Татьяна Ивановна

Межрайонный отдел судебных приставов по ИПНО города Москва

Адрес: 127083, Россия, Москва, ул. Мишина, д. 56, корп. 8,

Время работы: ВТ с 09.00 до 13.00 ЧТ с 13.00 до 18.00

Телефон для справок: +7(499)558-15-26

Телефон пристава-исполнителя: +7(499)558-15-26

Также были выявлены факты распространения модуля для удаленного управления через github.com, а в некоторых случаях использовались переименованные ссылки.


От: ООО СХП Раевское <raevckoe@mail.ru>
Кому: [redacted]
Копия:
Тема: Fwd[2]: Акт сверки и пп, счет
Акт сверки взаиморасчето...
1 файл Скачать (50 КБ) Сохранить в Облако
191227017 от 27.12.2019 (2...
1 файл Скачать (81 КБ) Сохранить в Облако
https://drive.google.com/open?id=1rJohEVDMa64ujmp8BDmcgvyNtVOa-5p2
С уважением,
ООО "СХП Раевское"

На первом этапе реализации атаки RTM обычно происходит проверка на отсутствие в запускаемой среде индикаторов средств анализа вредоносного кода и специально выделенных сред для безопасного выполнения исполняемых файлов.

Далее загрузчик основного модуля проверяет систему на наличие признаков того, что пользователь зараженного компьютера осуществляет взаимодействие с системами ДБО и бухгалтерского учета. Поиск осуществляется в том числе в истории браузеров и кэше интернет-страниц. Кроме того, в системе запускается модуль, предназначенный для копирования сохраненных паролей.

При наличии какого-либо признака финансовой деятельности на компьютер загружается основной модуль RTM. Причем периодически происходит смена адресов, по которым осуществляется загрузка основного модуля либо возвращение к ранее использовавшимся адресам. Адреса контрольных серверов не вшиты в тело основного модуля, а образуются динамически. Получение адресов контрольных серверов осуществляется путем формирования запросов через один или несколько блокчейн-обозревателей типа blockchain.info, blockcypher.com.

В процессе исследований, проводимых сотрудниками ФинЦЕРТ, было замечено несколько различных механизмов хищения денежных средств с применением RTM:

- Использование программ удаленного администрирования. Чаще всего применялся TeamViewer с дополнительной библиотекой, позволяющей запускать программу в скрытом режиме. Иногда использовались легальные программы, ранее установленные самими пользователями. В режиме удаленного администрирования операторы RTM подключались к системам ДБО и производили переводы денежных средств.
- Встраивание специального модуля в процесс веб-браузера. Вероятно, в таких случаях операторами осуществляется подмена платежных поручений в процессе их формирования при работе с веб-сайтами систем ДБО.
- Если для подключения к ДБО использовался сертификат, записанный на обычный отчуждаемый носитель, а не на защищенный токен, операторы копировали его. Затем получали пароли к ДБО с использованием встроенного кейлоггера и программы типа WebBrowserPassView (если пароль сохранен в браузере). Последующее формирование и отправка платежных поручений производились на стороннем компьютере с использованием сертификата и подключения к ДБО.

Так или иначе, данные механизмы были освоены группой после того, как производители бухгалтерского программного обеспечения изменили способ экспорта-импорта подготовленных платежных поручений и ранее активно использовавшийся механизм подмены реквизитов в платежных поручениях перестал работать.

Группа остается крайне эффективной, быстро меняет и легко осваивает новые тактики и техники атак, вносит изменения в инструментарий и по-прежнему остается главной опасностью для юридических лиц и индивидуальных предпринимателей. Отметим также, что рассылки по электронной почте являются не единственным способом распространения ВПО RTM. Специалисты ФинЦЕРТ регулярно проводят исследования носителей информации, подвергшихся воздействию данного ВПО, и выявляют случаи, когда проникновение произошло в результате посещения якобы легального сайта, содержащего образцы бухгалтерских документов.

Примечательно, что других серийных кампаний против клиентов ни в 2019 году, ни в последующий период участники информационного обмена не фиксировали. Специфика информационного обмена ФинЦЕРТ и поднадзорных организаций подразумевает в первую очередь передачу информации об угрозах самим организациям. Клиенты этих организаций не имеют возможности напрямую отправлять информацию об атаках в ФинЦЕРТ, и, следовательно, мы не можем владеть полностью ситуацией вне пределов действия поднадзорных организаций. Однако на большом объеме поступающих данных, а также в результатах исследований следы работы других групп были бы в любом случае заметны и какие-либо образцы используемого ими ВПО поступали бы. Таким образом, группа RTM остается не только особо опасной, но и представляет наиболее актуальную угрозу для клиентов финансовых организаций – юридических лиц и индивидуальных предпринимателей.

Атаки с использованием программ-шифровальщиков

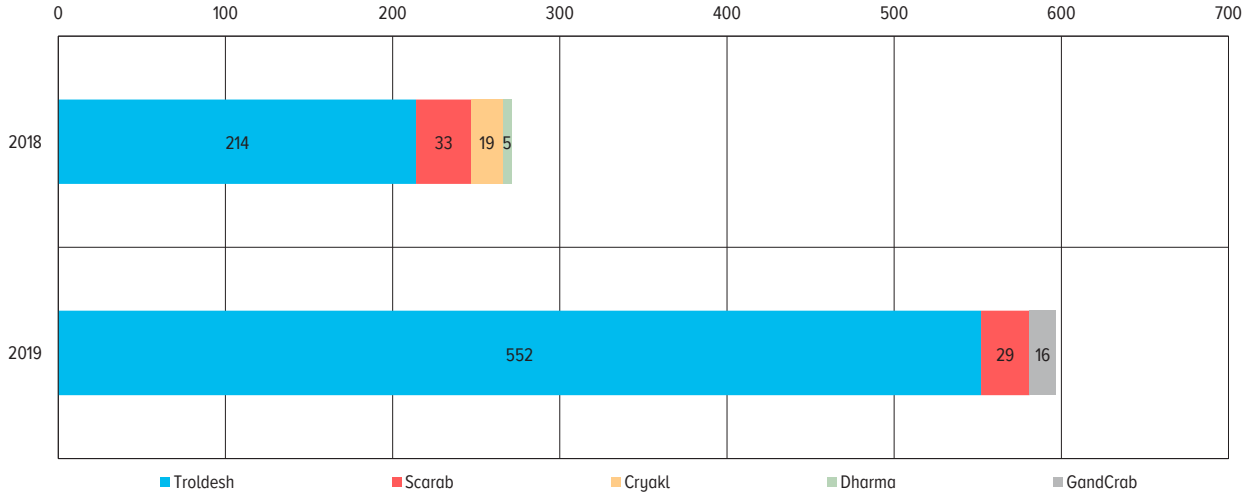
В 2019 году отмечалось большое количество запросов участников информационного обмена по фактам распространения различных программ-шифровальщиков.

Большая часть запросов была связана с распространением шифровальщиков семейства Troldesh (также известного как Shade или Purga). Потеснить в количественном отношении данную кампанию не смог и шифровальщик GandCrab, имевший широкое распространение по всему миру в 2019 году, но почти не отметившийся в рассылках на адреса организаций кредитно-финансовой сферы.

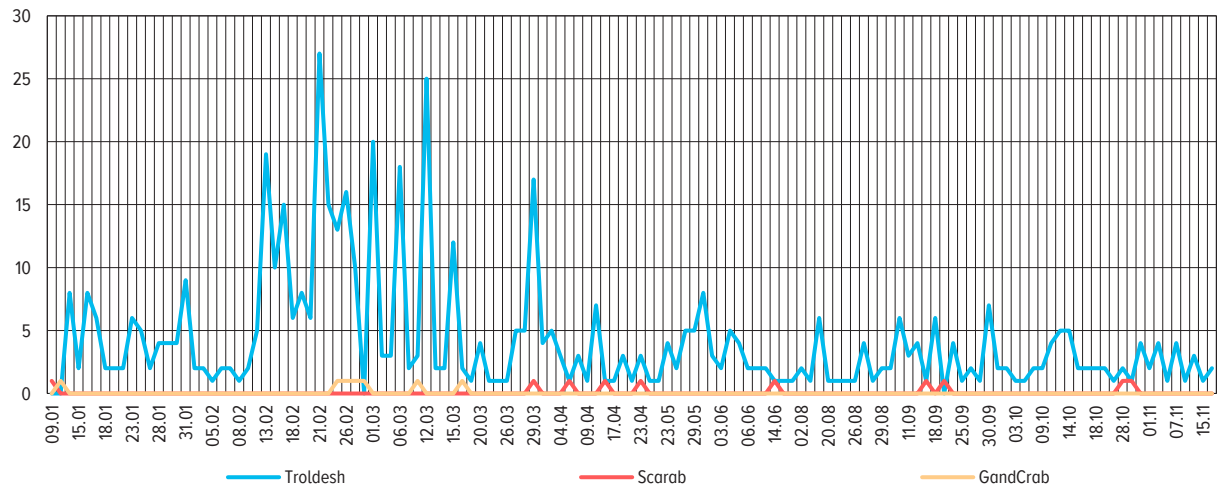
Основной способ распространения программ-шифровальщиков – рассылка по электронной почте сообщений, содержащих во вложении вредоносный исполняемый файл либо имеющих в тексте самого сообщения ссылку на скачивание данного файла.

В случае с Troldesh направляемые организациям сообщения использовали схожий стиль оформления: сообщения поступали якобы от имени организаций кредитно-финансовой сферы, авиакомпаний и крупных компаний иных отраслей. Часто в рассылке сообщений применялся спуфинг.

АТАКИ ПО ТИПАМ ШИФРОВАЛЬЩИКОВ *Рис. 7*
(ЕДИНИЦ)



ИНТЕНСИВНОСТЬ РАСПРОСТРАНЕНИЯ РАЗЛИЧНЫХ ПРОГРАММ-ШИФРОВАЛЬЩИКОВ В 2019 ГОДУ *Рис. 8*
(ЕДИНИЦ)



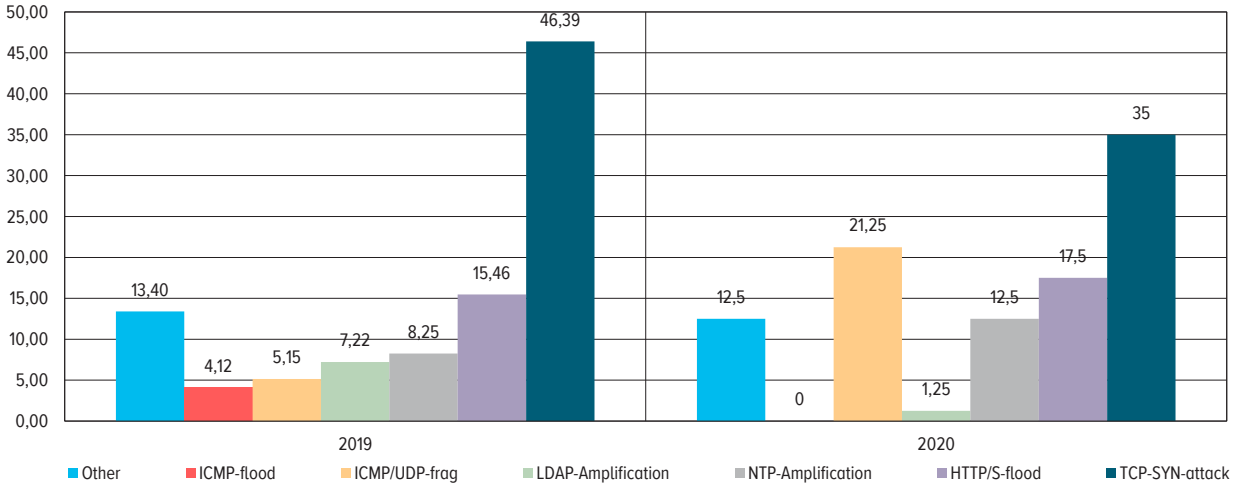
Однако длившаяся почти полтора года кампания по распространению шифровальщика Troldesh закончилась в декабре 2019 года. Его операторы перестали выпускать новые версии вымогателя и опубликовали около 750 тыс. ключей дешифрования, на основе которых затем были созданы дешифраторы. В 2020 году массовых кампаний больше не отмечалось и выявлялись лишь отдельные факты получения участниками информационного обмена ФинЦЕРТ рассылок с приложением программ-шифровальщиков.

Атаки типа «отказ в обслуживании»

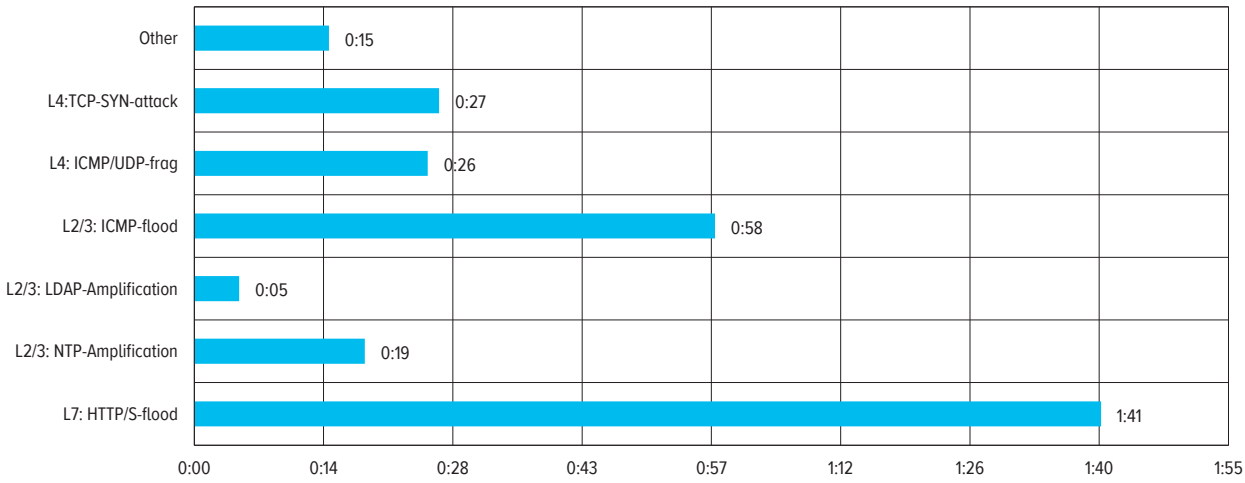
За отчетный период ФинЦЕРТ получил 221 сообщение от участников информационного обмена об инцидентах, связанных с атаками типа «отказ в обслуживании» (DoS).

В результате анализа полученных сообщений выявлен рост атак с типом TCP-SYN (SYN Flood, или атака «переполнения SYN-пакетами»). При атаке с помощью переполнения SYN-пакетами используется «трехстороннее рукопожатие» по протоколу TCP, чтобы вызвать сбои в работе сети и сервисов. Поскольку инициатором «трехстороннего рукопожатия» TCP всегда является клиент, то он первым отправляет пакет с флагом SYN серверу.

КОЛИЧЕСТВО DOS-АТАК С РАЗБИВКОЙ ПО ТИПАМ *Рис. 9*
(%)



СРЕДНЯЯ ПРОДОЛЖИТЕЛЬНОСТЬ АТАКИ *Рис. 10*
(ЧАСОВ)



Самые продолжительные атаки в отчетный период были зафиксированы именно с типом TCP-SYN. Длились они в 2019 году 11 часов 21 минуту, в 2020 году – 4 часа 18 минут. Несмотря на большую продолжительность атак, они не привели к нарушению доступности сервисов атакованных организаций. Самая большая продолжительность эффективного воздействия на сервисы организации была зафиксирована при совершении DoS-атаки с типом HTTP/S-flood – 1 час 41 минута.

По данным ФинЦЕРТ, самая мощная атака, выявленная в 2019–2020 годах, велась с интенсивностью 49 000 Мбит/с (49 Гбит/с), что на 2 Гбит больше рекорда 2018 года, когда мощность атаки составила 47 Гбит/с. Эта атака также не привела к нарушению доступности сервисов, предоставляемых организацией.

Если говорить о целевых объектах при DoS-атаках на финансовые организации, информация о которых поступала в ФинЦЕРТ в 2019–2020 годах, то чаще всего это системы ДБО и сервисы онлайн-банкинга, а также иные сервисы для осуществления переводов денежных средств. В результате реализации атак периодически происходило прерывание функционирования этих сервисов, что говорит о целенаправленном характере атак.

При этом из-за сложного взаимодействия финансовых сервисов внутри организаций при атаках часто наблюдались цепочки поочередных прерываний функционирования различных сервисов. К примеру, в ходе развития одной из атак на банк сначала стали недоступны все внешние ресурсы банка, у клиентов появились проблемы со входом в мобильную версию ДБО, далее был приостановлен поток обрабатываемых заявок от внешнего сервиса проведения платежей, возникли перебои в работе сервиса электронной коммерции, не проходили платежи через терминалы, а некоторые банкоматы оказались недоступны.

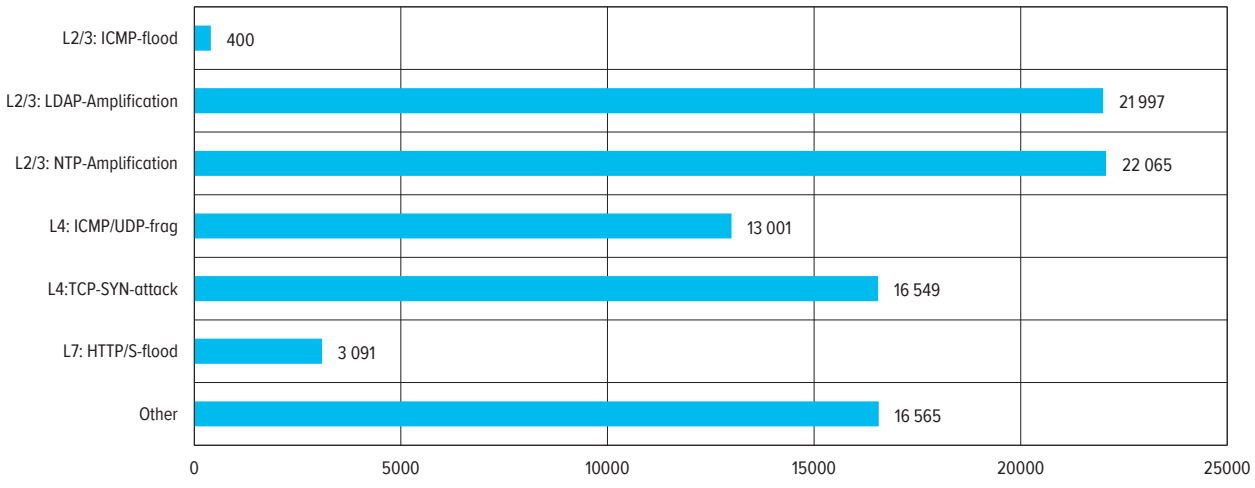
В ряде случаев фиксировались единичные специфические атаки небольшой мощности, направленные на формы авторизации веб-сайтов. Например, путем направления HTTP POST-запросов к форме авторизации клиентов ДБО банка с ограниченного диапазона IP-адресов. Целями таких атак может являться проверка возможности эксплуатации неких уязвимостей и слабостей в механизмах аутентификации и авторизации.

Еще одним интересным примером атаки на определенный сервис банка стала DoS-атака, которая привела к недоступности сервиса 3-D Secure в течение нескольких часов. Предположительно такая атака могла быть использована в сложной схеме проведения серии хищений денежных средств со счетов клиентов банка.

Среди зафиксированных ФинЦЕРТ Банка России в 2020 году DoS-атак можно выделить некоторые особенности и частные случаи. Так, например, были отмечены DoS-атаки прикладного уровня (L7), направленные на нарушение работы веб-приложений, которые сопровождались

СРЕДНЯЯ МОЩНОСТЬ АТАК
(MBPS)

Рис. 11



сканированием уязвимостей веб-сервисов. Проведение DoS-атак в этих случаях являлось хорошо известным приемом сокрытия в общем трафике следов работы сетевых сканеров уязвимостей, что может говорить о начальном этапе сложных целевых атак. Атаки прикладного уровня на веб-сервисы характеризуются максимальным таргетированием всех запущенных сервисов сайта. Другими словами, в ходе атаки достигается полное покрытие всех работающих сервисов и поддоменов сайта организации. Целью ее проведения является повышение эффективности реализации основной атаки и усложнение устранения ее последствий.

Атаки на банкоматы

ФинЦЕРТ в 2019–2020 годах получил 17 сообщений от участников информационного обмена о различных атаках на банкоматы.

На основе проведенного анализа было выявлено, что злоумышленники чаще всего (44% всех случаев) использовали различные приспособления для вскрытия (отжима) дверцы банкомата с последующим извлечением и хищением банкоматных кассет с денежными средствами.

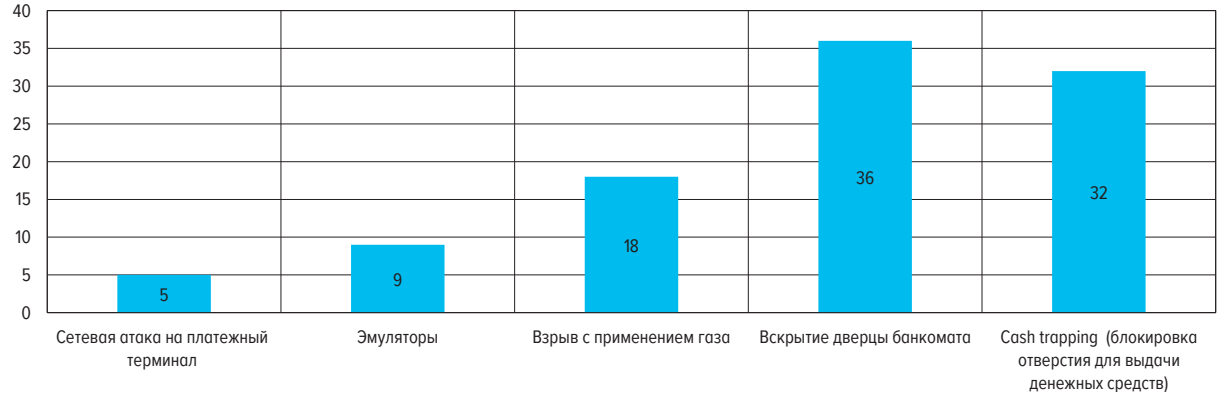
32% случаев связаны с кеш-треппингом (cash trapping), что дословно означает «захват наличности». Злоумышленники используют обычные алюминиевые планки, в большинстве случаев изготовленные из деталей мебельной фурнитуры. Металлическая планка, внешне похожая на шторку банкомата, с тыльной стороны клеится на двустороннюю клейкую ленту и крепится на отверстии выдачи наличных. Невнимательные граждане снимают наличные в банкомате с установленной планкой, не обратив внимание на его внешний вид. Когда операция по снятию проходит «с ошибкой», ничего не подозревающий гражданин просто уходит, думая, что банкомат неисправен. Затем злоумышленники подходят к банкомату и забирают наличные, приклеившиеся к тыльной стороне металлической планки.

В 2019 году была зафиксирована атака на банкомат с использованием Instrusion.Win.MS17-010. Атака проходила в течение четырех часов, однако была заблокирована средствами антивирусной защиты. Атака велась с зараженной рабочей станции, используемой для проведения технических обновлений платежного терминала.

Также в конце 2020 года в Дальневосточном федеральном округе были зафиксированы атаки с использованием ПО Cutlet Maker. Одна из них привела к хищению порядка 1,5 млн рублей. Атака стала возможной по причине нестабильной работы средств антивирусной защиты. В результате злоумышленники смогли подключить съемный носитель к банкомату и воспользоваться ПО, эмулирующим работу терминала, – Cutlet Maker.

Однако чаще всего (60% всех зафиксированных случаев) злоумышленники используют более «шумные» методы – газовые баллоны для проведения подрыва дверцы банкомата и иные средства физического воздействия с целью извлечения кассет с денежными средствами.

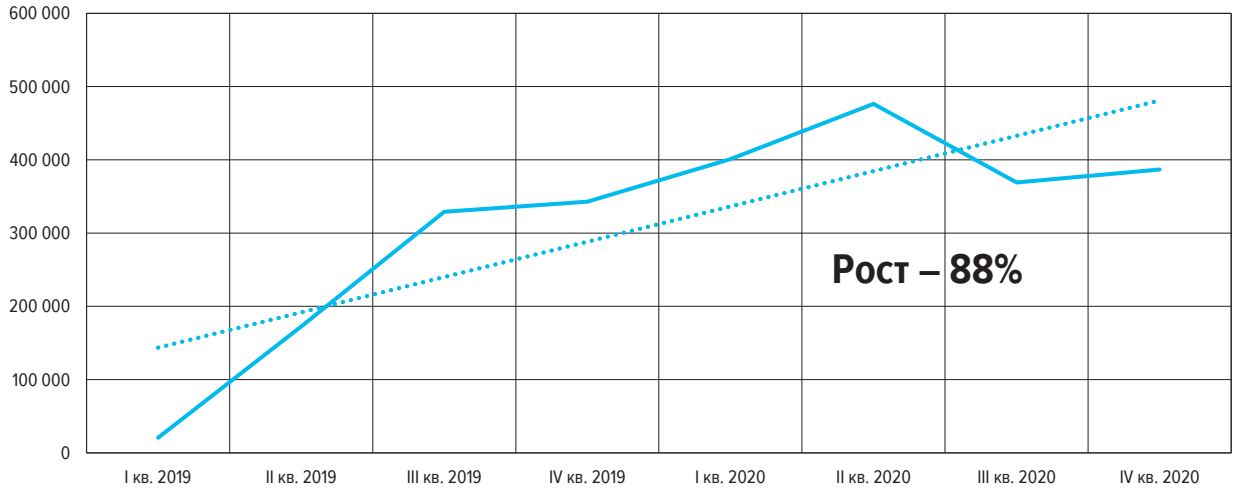
ВЫЯВЛЕННЫЕ ТИПЫ АТАК НА БАНКОМАТЫ, 2019–2020 ГОДЫ (%) *Рис. 12*



АТАКИ С ИСПОЛЬЗОВАНИЕМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В 2019–2020 ГОДАХ

Исходя из данных, полученных ФинЦЕРТ по каналам информационного обмена, на финансовом рынке наблюдается общая тенденция увеличения количества атак на клиентов кредитных организаций. Анализ сообщений, полученных от участников информационного обмена, показал, что за последние 12 месяцев общее количество инцидентов выросло на 88% по сравнению с 2019 годом.

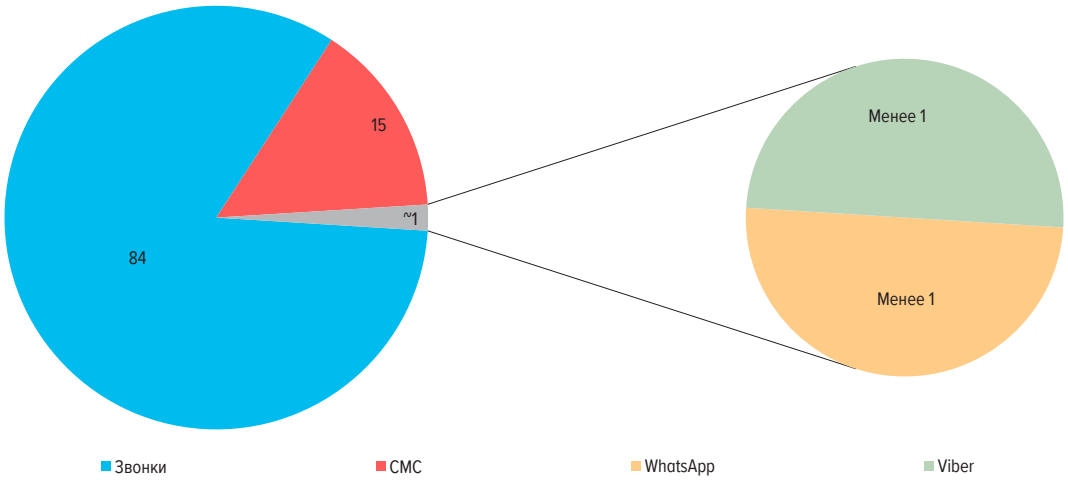
ОБЩЕЕ КОЛИЧЕСТВО ИНЦИДЕНТОВ, 2019–2020 ГОДЫ *Рис. 13*
(ЕДИНИЦ)



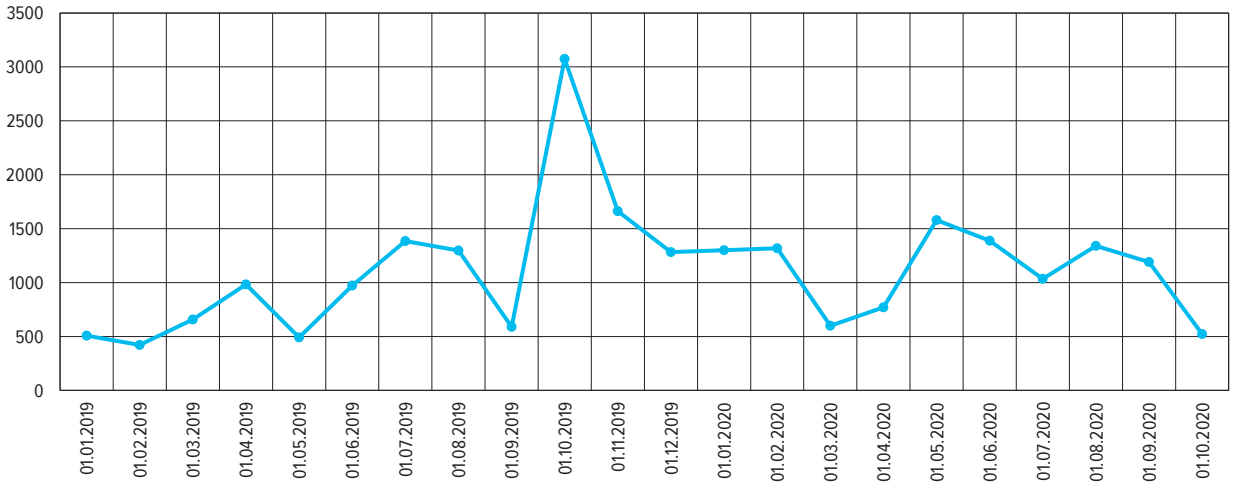
Типовые атаки с использованием методов социальной инженерии

В 2019–2020 годах злоумышленники использовали телефонную связь как канал воздействия на предполагаемую жертву в 84% случаев. Около 16% произошедших инцидентов связано с получением гражданами мошеннических СМС или сообщений в различных мессенджерах.

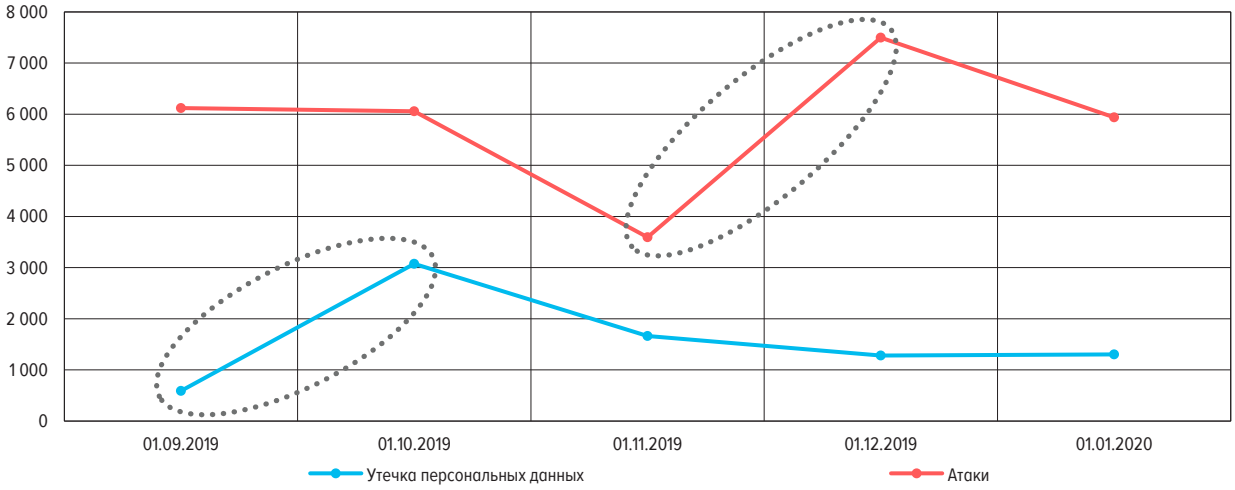
РАСПРЕДЕЛЕНИЕ АТАК НА ФИЗИЧЕСКИХ ЛИЦ ПО КАНАЛАМ ВОЗДЕЙСТВИЯ *Рис. 14*
(%)



КОЛИЧЕСТВО ИНФОРМАЦИОННЫХ СОБЫТИЙ В СМИ ПО ТЕМЕ «ХИЩЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ» *Рис. 15*
(ЕДИНИЦ)



ВЗАИМОСВЯЗЬ РОСТА УТЕЧЕК И АТАК *Рис. 16*
(ЕДИНИЦ)



В конце 2019 года основным трендом атак на организации финансовой сферы стали хищения персональных данных физических и юридических лиц для их дальнейшего использования в противоправных целях. Основной пик утечек пришелся на октябрь 2019 года.

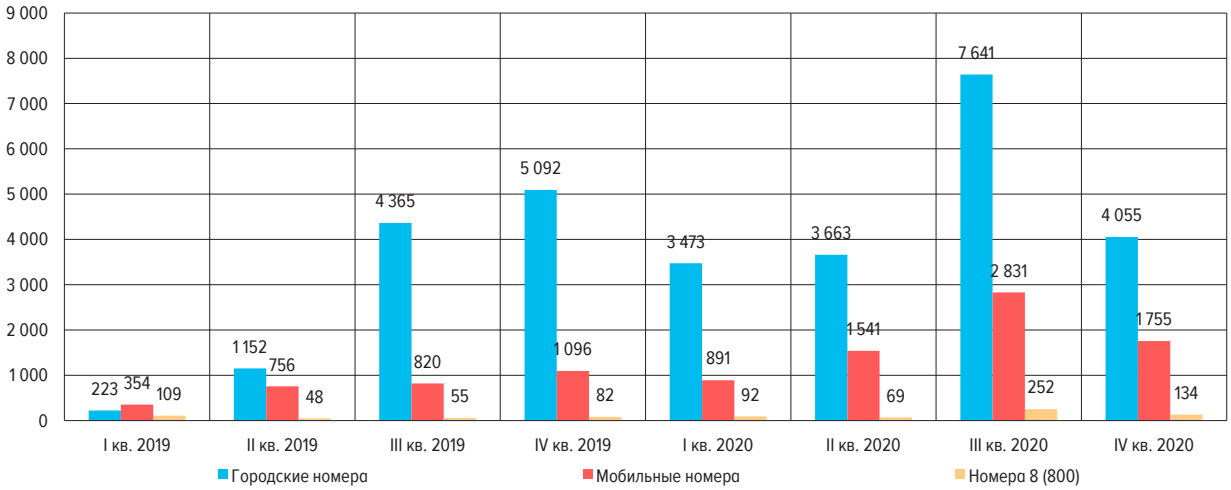
Резкий рост утечек персональных данных коррелируется с увеличением количества атак, связанных с использованием методов социальной инженерии – фишинга.

Стоит отметить, что хищение персональных данных, их последующая продажа, подготовка к массовым атакам по похищенным персональным данным вызвали некий лаг (отсрочку) в атаках. В период с ноября по декабрь 2019 года наблюдалось постепенное увеличение атак с пиком в декабре.

За 2020 год ФинЦЕРТ направил на блокировку операторам связи 26 397 телефонных номеров, что превышает показатель предыдущего года на 86%.

ФинЦЕРТ провел анализ характера звонков – кем представляются злоумышленники при звонках гражданам. Выяснилось, что в большинстве случаев (порядка 57%) мошенники представляются сотрудниками службы безопасности той или иной финансовой организации, а также просто сообщают, что звонят из кредитной организации, обслуживающей счет гражданина (41% случаев). С конца 2020 года ФинЦЕРТ также наблюдает существенный рост числа инцидентов, связанных со звонками злоумышленников от имени сотрудников правоохранительных органов.

КОЛИЧЕСТВО МОШЕННИЧЕСКИХ ТЕЛЕФОННЫХ НОМЕРОВ, НАПРАВЛЕННЫХ ФИНЦЕРТ ОПЕРАТОРАМ СВЯЗИ (ЕДИНИЦ) *Рис. 17*

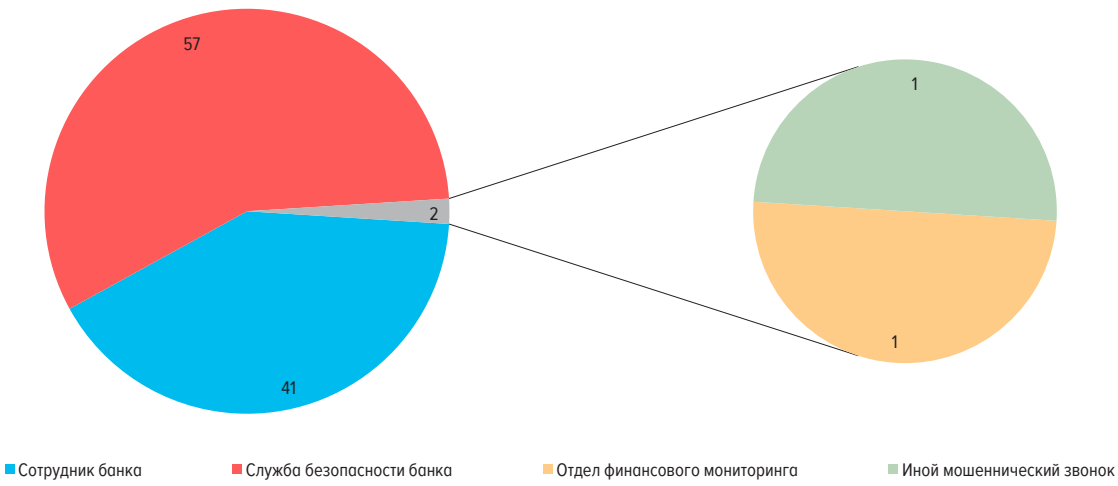


Злоумышленники также используют канал электронных сообщений (СМС, мессенджеры) при совершении мошеннических действий на таких сервисах, как «Юла» или «Авито». По данным ФинЦЕРТ, в большинстве случаев (около 83%) мошенники используют переписку с потерпевшим для псевдопокупки/продажи товаров или услуг. 15% всех инцидентов приходится на мошеннические СМС-сообщения с информацией о блокировке карты.

Условия пандемии способствовали росту количества мошеннических сайтов в кредитно-финансовой сфере. Данный рост обусловлен увеличением использования дистанционных сервисов и услуг, а также тем, что многие люди потеряли работу. Это повысило их потребность в социальных выплатах и вызвало интерес к кредитным продуктам и иным способам улучшения финансового положения. Злоумышленники активно используют тему коронавируса с целью создания сайтов лжебанков и иных фишинговых ресурсов для хищения денежных средств граждан. С марта по май (то есть в период максимально строгого локдауна) было выявлено 2200 мошеннических сайтов, создатели которых эксплуатировали тему коронавируса для обмана граждан. Величина аудитории мошеннических ресурсов резко возросла и составляет порядка 100 тыс. человек в сутки.

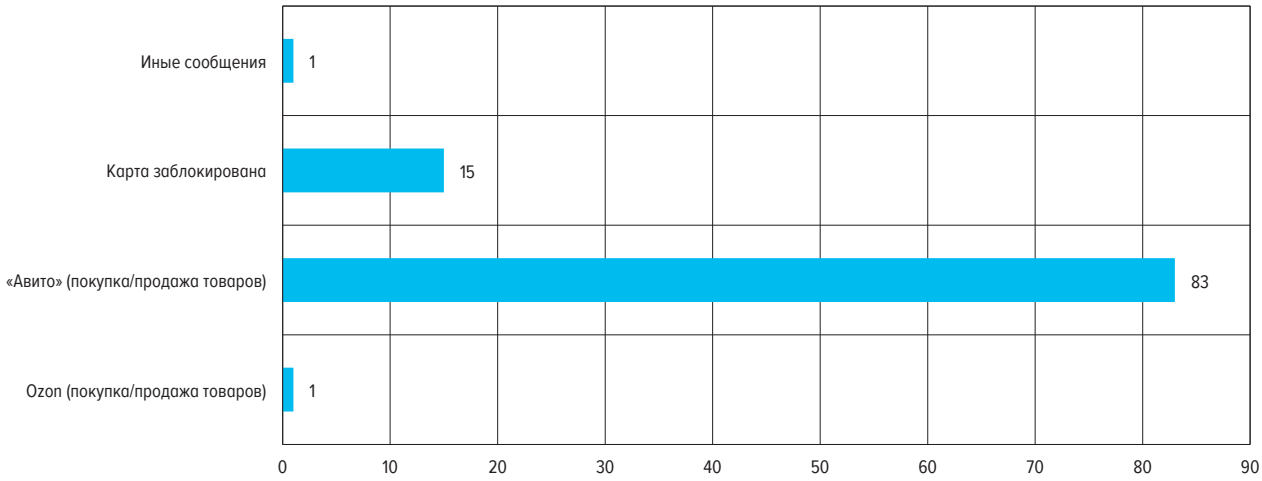
Всплеск количества информационных событий в СМИ совпадает с увеличением числа фишинговых ресурсов в сети Интернет, целью которых, как известно, является получение

КЕМ ПРЕДСТАВЛЯЮТСЯ МОШЕННИКИ (%) *Рис. 18*



РАСПРЕДЕЛЕНИЕ ПО СЦЕНАРИЯМ ВОЗДЕЙСТВИЯ
(%)

Рис. 19



конфиденциальных/персональных сведений граждан для дальнейшего их использования в противоправных целях. Тематика злоумышленниками также подбирается в соответствии с инфоповодами, которые активно распространяются через СМИ, социальные сети и так далее.

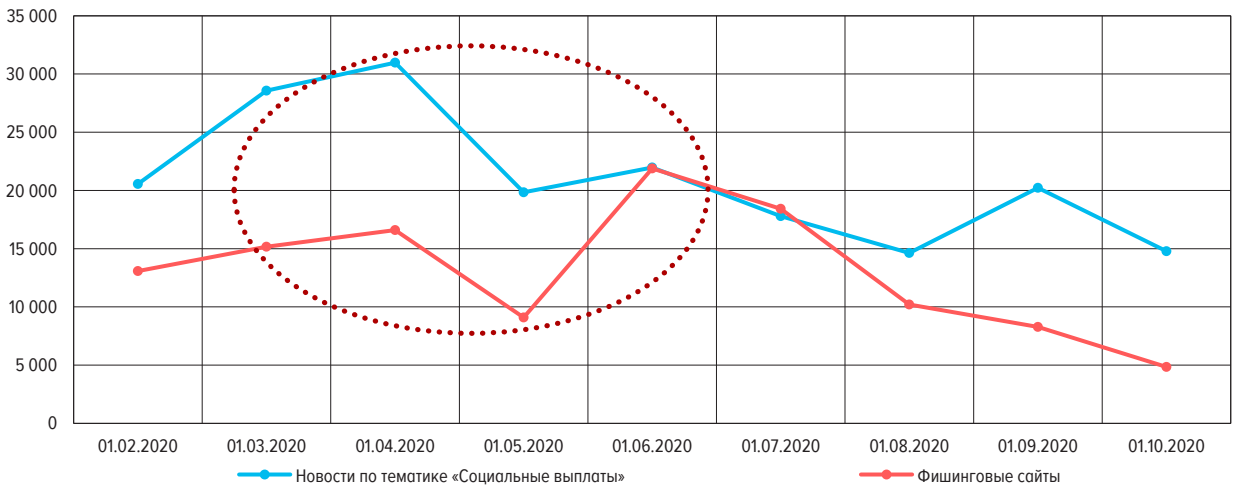
В современных эпидемических условиях, сложившихся в России, возрастает количество компьютерных атак, а также появляются новые риски в кредитно-финансовой сфере. Прежде всего это объясняется тем, что ввиду пандемии люди были переведены на режим самоизоляции, и это обусловило необходимость более активного использования дистанционного формата приобретения товаров, выполнения работ и оказания услуг.

Большинство организаций, в том числе в финансовой сфере, переориентировались на работу в дистанционном режиме, что не только позволило обеспечивать потребности граждан, но и перестроило работу злоумышленников. В период борьбы с COVID-19 ФинЦЕРТ зафиксировал значительный рост количества фишинговых рассылок, а также мобильного мошенничества.

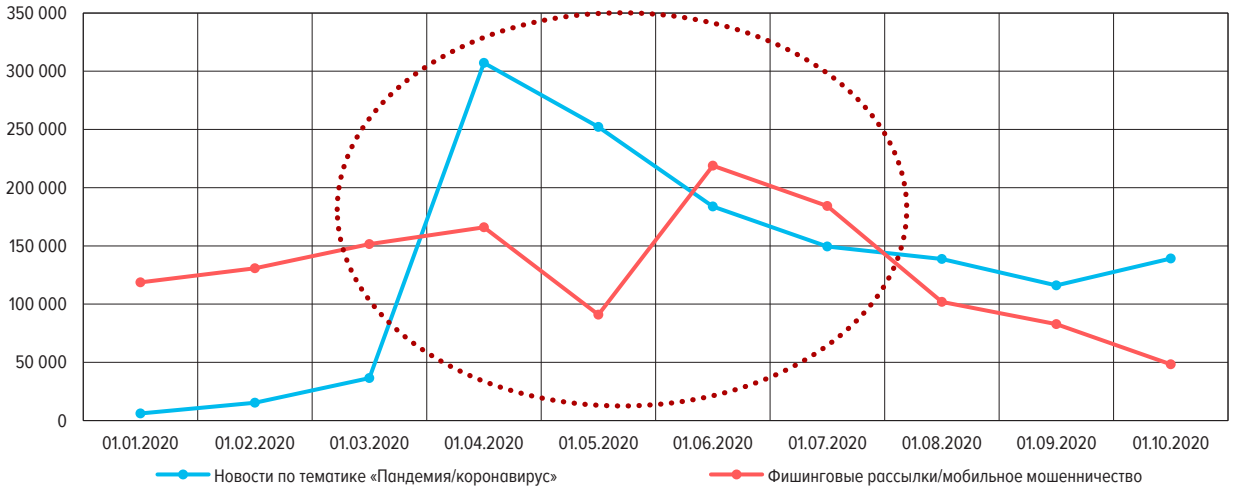
Спад активности злоумышленников в наблюдаемый период пришелся на май (до уровня январских значений по количеству инцидентов), что в целом соответствует сезонным колебаниям в связи с майскими праздниками.

КОРРЕЛЯЦИЯ КОЛИЧЕСТВА ИНФОРМАЦИОННЫХ ПОВОДОВ И ФИШИНГОВЫХ РЕСУРСОВ
(ЕДИНИЦ)

Рис. 20



КОРРЕЛЯЦИЯ КОЛИЧЕСТВА ИНФОРМАЦИОННЫХ ПОВОДОВ И АКТИВНОСТИ ПРЯМЫХ АТАК (ЕДИНИЦ) *Рис. 21*



Показатели июня также подтверждают данную статистику – резкий рост фишинговых ресурсов, связанных с различными псевдовыплатами, социальной поддержкой государства, налогами. Фишинговые ресурсы и мобильное мошенничество с применением методов социальной инженерии направлены прежде всего на незащищенные слои населения, а также на тех людей, которые в период пандемии столкнулись с тяжелой финансовой ситуацией в связи с утратой источника дохода (увольнением, сокращением, закрытием бизнеса и так далее).

Образ типичного мошенника и жертвы при атаке с использованием социальной инженерии

Обладая персональными данными жертвы, мошенники могут с легкостью представляться сотрудниками как финансовых, страховых организаций, так и государственных органов, чем вводят собеседника в заблуждение. Клиент, считая, что указанные данные могут быть известны только ему или организации, поддается на обман, сообщая в конечном итоге контрольные слова, коды подтверждения и другие данные, предоставляющие мошенникам возможность вывести денежные средства с подконтрольных клиенту счетов.

Злоумышленники, как правило, представляются сотрудниками финансовых организаций или сотрудниками органов государственной власти и государственных фондов, как это происходило в период пандемии. В процессе разговора слышится фоновый шум колл-центра – это позволяет создать иллюзию, что лицо, которое осуществило звонок, является сотрудником крупной организации. Затем мошенники, как правило, переносят жертву в ситуацию быстрого выбора действий, при которой человеку необходимо принять решение в минимальные сроки, чтобы «спасти» денежные средства, которые пытаются похитить. При этом злоумышленники стараются не терять контакт с жертвой, не дают возможности подумать, проанализировать ситуацию или перезвонить.

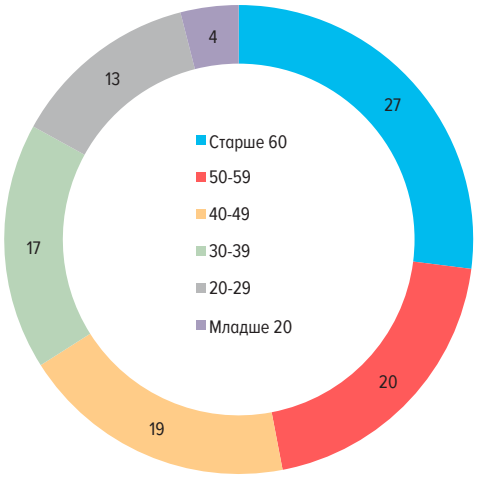
Источником данных стали экспертные интервью руководителей служб информационной безопасности крупнейших банков, основанные на данных, полученных в результате анализа заявлений клиентов и клиентской базы кредитных организаций.

Условно среди жертв социальной инженерии можно выделить следующие основные группы:

- «Индивидуалисты» – благополучные в финансовом плане, легко тратят на себя и удовольствия, излишне доверяют новым технологиям.
- «Школьники, студенты, лица с особенностями социальной адаптации» – доверчивые, расточительные, импульсивные, склонные к риску, противоречивая самоидентификация.

ВОЗРАСТ ЖЕРТВ
(%)

Рис. 22



- «Бюджетораспорядители семей с невысоким уровнем дохода и высокой финансовой нагрузкой» – целеустремленные, высоко ценят семейные и дружеские связи, ответственные.
- «Домохозяйки» – уступчивые, доверчивые, внешний локус контроля.
- «Серебряный возраст» – возраст 60+.

На схеме видно, что треть жертв социальной инженерии составляют граждане старше 60 лет. Однако вызывает беспокойство тот факт, что основной удар приходится на экономически активное население в возрасте 20–60 лет. Также установлено, что чаще всего жертвами мошенников становятся женщины (более 65%).

Противодействие атакам с использованием социальной инженерии

Противодействие совершению операций без согласия клиента является одной из приоритетных задач деятельности Департамента информационной безопасности и ФинЦЕРТ в его составе.

Для реализации указанной задачи Банком России сформирована нормативно-правовая база, в том числе предусматривающая обязанность финансовых организаций по проведению антифрод-процедур, которые согласно нормам закона реализуются в рамках систем управления рисками банков, и аутентификации клиентов. Банком России созданы технические условия обмена информацией для проведения банками антифрод-процедур.

В 2019 году был отмечен массовый рост числа звонков клиентам банков якобы от имени сотрудников финансовых организаций. Под предлогом остановки операции, совершаемой без согласия клиента, злоумышленники выпытывали у жертв данные карт, коды из СМС и другую информацию, способствовавшую совершению хищения средств. Указанные подходы не используют технику эксплуатации уязвимостей в банковских технологических процессах и программно-технических средствах.

Объем всех операций с использованием электронных средств платежа (ЭСП), совершенных без согласия клиентов, в 2019 году составил 6426,5 млн руб., количество таких операций – 576 566 единиц. 69% всех операций без согласия совершено в результате побуждения клиентов к самостоятельному проведению операции путем обмана или злоупотребления доверием методами социальной инженерии.

В качестве одного из основных направлений противодействия такому мошенничеству определено развитие культуры информационной безопасности и кибергигиены клиентов – потребителей банковских услуг.

В рамках данного направления реализованы следующие мероприятия:

1. Проведен анализ социально-демографических характеристик категорий граждан, наиболее восприимчивых к приемам социальной инженерии[1]. На основе результатов разработаны таргетированные информационные материалы для распространения в целях повышения уровня культуры информационной безопасности.
2. Проведены информационные кампании в СМИ и социальных сетях, включающие публикации популярных блогеров и распространение предупреждающих материалов в различных сообществах.
3. Разработаны и продвигаются тематические материалы на сайте *«Финансовая культура»*.
4. Проведено обучение 920 работников правоохранительных органов по вопросам противодействия совершению операций без согласия клиента[2].
5. Размещена социальная реклама в общественных местах.

В 2020 году основным фактором, определявшим ландшафт угроз информационной безопасности при совершении операций клиентами организаций финансового сектора, стал рост объема операций с использованием ЭСП, в первую очередь CNP-транзакций при оплате товаров и услуг через Интернет. Как следствие, выросли и количественные показатели операций без согласия клиента.

Необходимо подчеркнуть, что Российская Федерация, по данным международных платежных систем, не входит в число стран – лидеров по уровню мошенничества в мире.

Анализ представленной выше статистики позволяет сделать следующие выводы:

- социальная инженерия является основной причиной совершения операций без согласия клиента (мошеннических операций);
- проводимые мероприятия по повышению культуры информационной безопасности и кибергигиены способствуют снижению уровня операций без согласия клиентов, но для достижения более значимого результата требуется активизация этой работы;
- отмечается крайне низкая доля возврата денежных средств клиентам[3].

Проведенный анализ международного опыта показывает, что методы, которые используют злоумышленники, сильно зависят от уровня развития платежных инструментов и применяемых платежных технологий в стране. Реализация методов социальной инженерии путем массовых телефонных звонков клиентам финансовых организаций характерна в значительной степени для Российской Федерации и не имеет широкого распространения в других странах. Более того, схемы телефонного мошенничества, отработанные в Российской Федерации, далее транслируются на территории государств ЕАЭС и СНГ.

Возможность применения методов социальной инженерии обусловлена следующими факторами:

1. Нелегальный оборот персональных данных, которые используются для организации массовых звонков клиентам банков. Источниками этих данных могут являться не только банки (например, отмечены существенные утечки данных о покупках с применением платежных карт в интернет-магазинах).

---

[1] По данным Департамента информационной безопасности на конец 2019 года, жертвами злоумышленников чаще всего становятся пенсионеры и женщины, ведущие домашнее хозяйство. Значительная доля объема операций без согласия приходилась также на благополучных в финансовом плане граждан, которые теряли крупные суммы, рассчитывая заработать или поддавшись на угрозу потери всех средств, находящихся на банковских счетах.

[2] Практико-ориентированное обучение по вопросам информационной безопасности проводится в соответствии с резолюцией Председателя Банка России от 13 июля 2020 года № ВН-014-56-3/1586.

[3] Кредитные организации не возвращают денежные средства в случае нарушения клиентом условий договора с кредитными организациями, предусматривающих необходимость сохранения конфиденциальности платежной информации (статья 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе»).

2. Использование злоумышленниками скриптов взаимодействия КО с клиентами – например, аналогичных получению банком у клиента опровержения или подтверждения подозрительных операций.
3. Перенос банками рисков на клиентов в соответствии с текущей редакцией Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе».
4. Схема организации правонарушений предполагает существенные сложности для правоохранительных органов в определении организаторов преступлений. Отмечаются успешные практики выявления и задержания лиц, непосредственно задействованных в снятии денежных средств в банкоматах. Однако определить организаторов преступлений на основании технических данных или показаний задержанных во многих случаях не представляется возможным. Это позволяет организаторам преступлений вовлекать новых исполнителей, ранее не замеченных в противоправных действиях, что делает неэффективными процедуры KYC на стороне банков.

Банк России продолжает работу по борьбе с социальной инженерией в рамках проработки нормативных инициатив по следующим направлениям:

- борьба с нелегальным оборотом персональных данных;
- создание стимулов для банков в повышении качества антифрод-процедур;
- создание условий для повышения эффективности деятельности правоохранительных органов;
- расширение аудитории программ киберграмотности, ориентированных на целевые группы клиентов – физических лиц, с целью доведения информации до каждого клиента – физического лица.

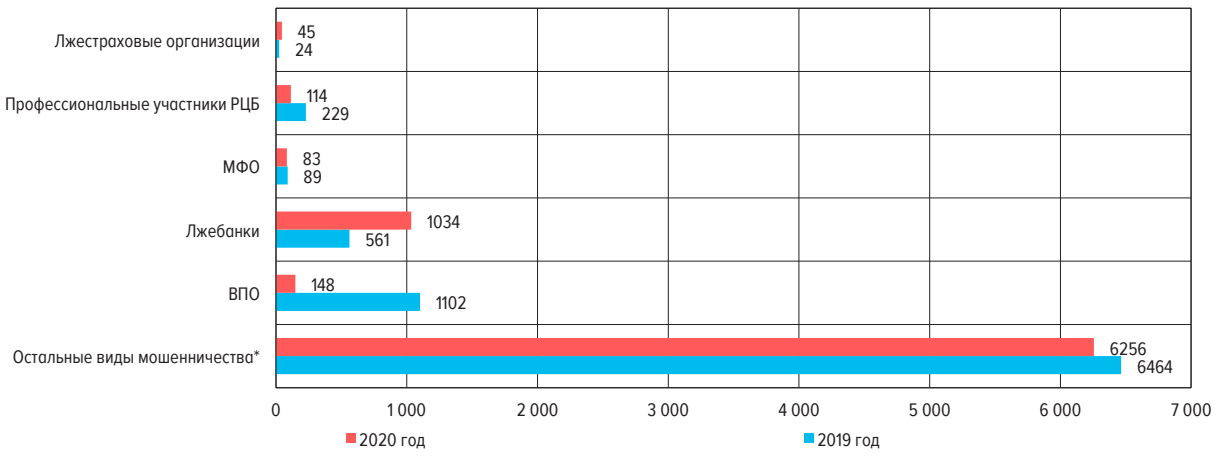
Противодействие мошенническим ресурсам

ФинЦЕРТ уведомляет регистраторов доменных имен о доменах, с которых рассылается вредоносный код и осуществляются мошеннические действия, связанные с использованием платежных карт.

Среднее время разделегирования доменов регистратором занимает от трех часов до трех дней.

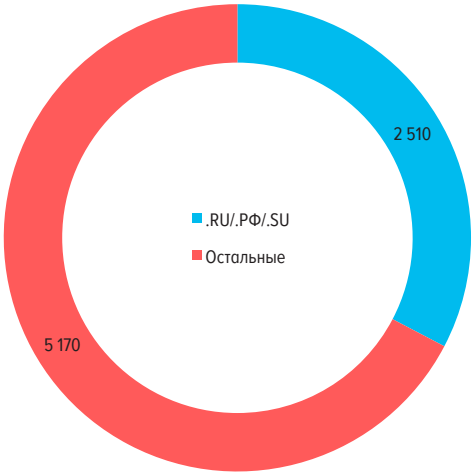
В 2019 году и в начале 2020 года ФинЦЕРТ направлял на блокировку преимущественно мошеннические сайты, маскирующиеся под страховые организации, продажу авиа/железнодорожных билетов, p2p-переводы, обменники, а также домены сайтов с ВПО. Всего в 2019 году было заблокировано 8 469 доменов.

БЛОКИРОВКА МОШЕННИЧЕСКИХ РЕСУРСОВ, 2019–2020 ГОДЫ *Рис. 23*
(ЕДИНИЦ)



** Продажа авиа/железнодорожных билетов, p2p-переводы, обменники и т.д.*

ЗОНЫ РАЗДЕЛЕГИРОВАНИЯ ДОМЕНОВ В 2020 ГОДУ *Рис. 24*
(ЕДИНИЦ)



В 2020 году Банк России инициировал блокировку 7680 сайтов. Основное большинство (6256 единиц), как и годом ранее, составляли мошеннические сайты, маскирующиеся под продажу авиа/железнодорожных билетов, p2p-переводы, обменники. Помимо них, были заблокированы 1034 сайта лжебанков и 45 сайтов лжестраховых организаций (по данным категориям был отмечен двукратный рост количества). 114 ресурсов было заблокировано в категории «Профессиональные участники рынка ценных бумаг» (двукратное снижение количества), 83 – в категории МФО, 148 – в категории сайтов с ВПО (их число снизилось в 7,5 раза по сравнению с 2019 годом).

ФинЦЕРТ активно реализует меры по противодействию противоправной деятельности в сети Интернет как в российских национальных, так и в иностранных доменных зонах. В 2020 году в доменных зонах .RU, .РФ, .SU инициировано снятие с делегирования 2510 доменов, в остальных зонах – 5170.

Запросы на разделегирование фишинговых ресурсов, в отношении которых у ФинЦЕРТ нет соответствующих компетенций (ресурс находится вне доменных зон .RU, .РФ, .SU), а также геодоменов, направляются в адрес компетентных организаций для организации содействия по снятию с делегирования доменов. В настоящее время Банком России совместно с Генеральной прокуратурой Российской Федерации проводится работа по обмену информацией о сайтах, выявленных в сети Интернет и используемых для совершения мошеннических действий в финансовой сфере, с целью последующего ограничения доступа к ним в соответствии со статьей 15.3 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В целях противодействия мошенническим ресурсам ФинЦЕРТ взаимодействует с антивирусными лабораториями и ГосСОПКА.

За прошедшие два года в рамках взаимодействия с вышеуказанными организациями антивирусным лабораториям было направлено 553 554 доменных имени, задействованных в распространении ВПО, ГосСОПКА – 755 508 доменных имен, задействованных в осуществлении фишинга и распространении ВПО.

ТРАНСФОРМАЦИЯ ТЕХНОЛОГИЙ АТАК В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ РОССИЙСКОЙ ФЕДЕРАЦИИ В ПЕРИОД РАСПРОСТРАНЕНИЯ КОРОНАВИРУСНОЙ ИНФЕКЦИИ В 2020 ГОДУ

Охватившая в 2020 году мир эпидемия коронавирусной инфекции (COVID-19) внесла существенные изменения почти во все сферы жизнедеятельности. Разумеется, они не могли не затронуть и криминальную ситуацию в кредитно-финансовой сфере. Главная цель всех наблюдаемых атак осталась без изменений – монетизация полученных результатов любым способом. Но набор средств и методов атак, их соотношение в арсеналах преступных групп ситуативно меняются под влиянием внешней обстановки.

В условиях распространения коронавирусной инфекции на территории Российской Федерации в марте 2020 года был зафиксирован рост числа кибератак на различные сервисы дистанционного обслуживания. Основная причина такого роста – введение большинством организаций кредитно-финансовой сферы режима удаленной работы. Многие граждане находились дома (на самоизоляции) и активно использовали банковские приложения для оплаты различных услуг – этому способствовало временное закрытие филиалов банков, МФО, введение штрафов за нарушение требований самоизоляции.

В период борьбы с COVID-19 Банк России зафиксировал (в сравнении с аналогичным периодом прошлого года):

- значительный рост количества фишинговых рассылок;
- появление новых видов вредоносного программного обеспечения;
- активизацию хакерских группировок.

Злоумышленники переориентировали свою деятельность на использование программ-шпионов с целью осуществления удаленного доступа к информационным системам организаций и последующего получения данных компаний для извлечения материальной выгоды. Прежде всего это связано с тем, что большинство организаций перешли на удаленный режим работы. Так, в 2020 году по сравнению с 2019 годом был зафиксирован двукратный рост использования шпионских программ.

Прогнозируя рост количества массовых рассылок ВПО и компьютерных атак на фоне перехода на дистанционный режим работы, Банк России выпустил информационное письмо «О мерах по обеспечению киберустойчивости и информационной безопасности в условиях распространения новой коронавирусной инфекции (COVID-19)» (от 20.03.2020 № ИН-014–56/17), а также подготовил и разослал 39 информационных бюллетеней о возможных атаках и методах противодействия им. Вместе с тем с учетом разработанных Банком России мер и рекомендаций по обеспечению информационной безопасности в условиях пандемии их повсеместное изучение и применение кредитными организациями обеспечили подготовку информационной инфраструктуры кредитных организаций к дистанционной работе. Принятые Банком России меры позволили избежать материального ущерба для организаций финансовой сферы от компьютерных атак в условиях перестройки операционной деятельности в период пандемии.

История коронавирусной трансформации мира еще не закончена, однако ФинЦЕРТ полагает необходимым отметить основные наблюдаемые тенденции.

Компьютерные атаки в период пандемии

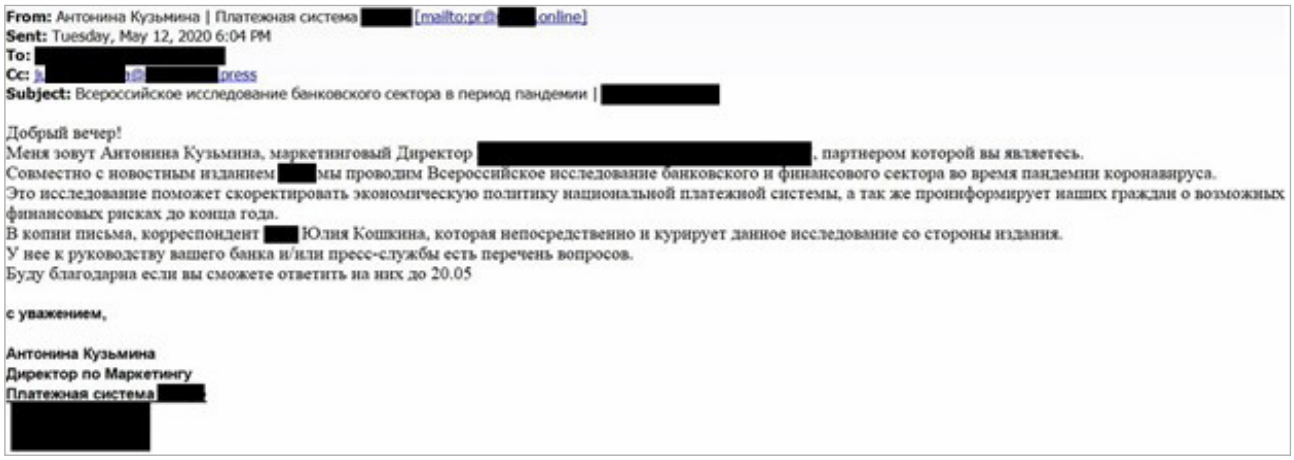
Отмечены следующие особенности компьютерных атак на инфраструктуру финансовых организаций и их клиентов, наблюдавшихся в течение периода карантина.

Во-первых, полностью перестали фиксироваться атаки ранее известных групп и/или атаки с использованием их традиционных для последних лет инструментов Buhtrap, Cobalt Strike, Silence и иных. При этом отмечено появление как минимум одной новой группы, активно совмещающей методы социальной инженерии и использование ВПО.

Во-вторых, имеются основания предполагать появление высококвалифицированной группы, специализирующейся на глубоком анализе мобильных приложений для дистанционного банковского обслуживания в целях обнаружения и эксплуатации слабостей и уязвимостей.

В-третьих, в общем потоке поступающих в ФинЦЕРТ от участников информационного обмена образцах вредоносного кода почти полностью исчезли программы-шифровальщики (ransomware) и стали преобладать программы класса шпионского ВПО (spyware), что демонстрирует значительно возросший спрос криминальной индустрии на конфиденциальные данные финансовых и не только организаций, их сотрудников и клиентов. Рассмотрим тенденции подробнее.

Первая тенденция – появление группы, активно совмещающей методы социальной инженерии и использование ВПО – представляется весьма угрожающей. Так, в мае 2020 года несколько российских финансовых организаций получили сообщения с темой «Всероссийское исследование банковского сектора в период пандемии I <наименование платежной системы> & <наименование информационного агентства>» с фиктивным указанием платежной системы в качестве отправителя.



From: Антонина Кузьмина | Платежная система [redacted] [mailto:pr@[redacted].online]
Sent: Tuesday, May 12, 2020 6:04 PM
To: [redacted]
Cc: [redacted]press
Subject: Всероссийское исследование банковского сектора в период пандемии | [redacted]

Добрый вечер!
Меня зовут Антонина Кузьмина, маркетинговый Директор [redacted], партнером которой вы являетесь.
Совместно с новостным изданием [redacted] мы проводим Всероссийское исследование банковского и финансового сектора во время пандемии коронавируса.
Это исследование поможет скорректировать экономическую политику национальной платежной системы, а так же проинформирует наших граждан о возможных финансовых рисках до конца года.
В копии письма, корреспондент [redacted] Юлия Кошкина, которая непосредственно и курирует данное исследование со стороны издания.
У нее к руководству вашего банка и/или пресс-службы есть перечень вопросов.
Буду благодарна если вы сможете ответить на них до 20.05

с уважением,

Антонина Кузьмина
Директор по Маркетингу
Платежная система [redacted]
[redacted]

Данное письмо не содержало вредоносных вложений и было предназначено для пробуждения интереса и фиксации воспоминаний. Через несколько дней получателям поступало второе сообщение в рамках данной кампании, в качестве отправителя значился якобы корреспондент одного из крупных информационных агентств.

From: [redacted]press [mailto:[redacted]
Sent: Wednesday, May 13, 2020 4:54 PM
To: [redacted]
Cc: Антонина Кузьмина | Платежная система [redacted]
Subject: Re: Всероссийское исследование банковского сектора в период пандемии I [redacted]

Добрый день, коллеги. Простите за задержку с ответом, завершала предыдущий материал к публикации.
Антонина, благодарю за вступительное письмо.
Скажите, вы сможете поучаствовать в нашем исследовании?
В случае положительного ответа, следующим письмом пришлю детали.

12 мая 2020 г., 18:03 Антонина Кузьмина | Платежная система [redacted] <pr@[redacted].online> пишет:

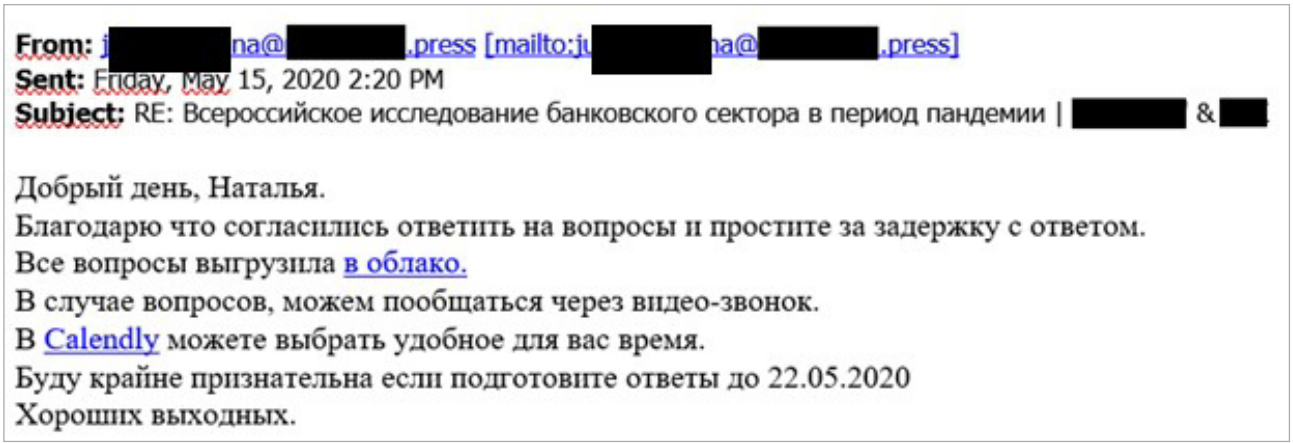
Добрый вечер!
Меня зовут Антонина Кузьмина, маркетинговый Директор [redacted], партнером которой вы являетесь.
Совместно с новостным изданием [redacted] мы проводим Всероссийское исследование банковского и финансового сектора во время пандемии коронавируса.
Это исследование поможет скорректировать экономическую политику национальной платежной системы, а так же проинформирует наших граждан о возможных финансовых рисках до конца года.
В копии письма, корреспондент [redacted] Юлия Кошкина, которая непосредственно и курирует данное исследование со стороны издания.
У нее к руководству вашего банка и/или пресс-службы есть перечень вопросов.
Буду благодарна если вы сможете ответить на них до 20.05

с уважением,

Антонина Кузьмина
Директор по Маркетингу
[redacted]

с уважением,
Корреспондент [redacted]
Юлия Кошкина
[redacted]

Если адресат продолжал переписку – а некоторые именно так и сделали – дальнейшие сообщения атакующих уже содержали ссылки на скачивание файлов с полезной нагрузкой. При этом ВПО было размещено на легальных ресурсах firefox [.] com и yadi [.] sk.


From: [redacted].press [mailto:[redacted].press]
Sent: Friday, May 15, 2020 2:20 PM
Subject: RE: Всероссийское исследование банковского сектора в период пандемии | [redacted] & [redacted]

Добрый день, Наталья.
Благодарю что согласились ответить на вопросы и простите за задержку с ответом.
Все вопросы выгрузила в облако.
В случае вопросов, можем пообщаться через видео-звонок.
В Calendly можете выбрать удобное для вас время.
Буду крайне признательна если подготовите ответы до 22.05.2020
Хороших выходных.

Устанавливаемая вредоносная программа запускала powershell для подключения к workers.dev – сервису сервлетов от Cloudflare, использованному в качестве интерфейса контрольно-командного сервера ВПО. Легальные ресурсы для распространения и управления ВПО задействовались для затруднения их блокировки – иногда трудно заблокировать поддомен, отдельный IP или URL без основного верхнеуровневого домена и/или всего адресного пространства большого легального ресурса, активно используемого в повседневной работе. Кроме того, использование подобного сервиса сервлетов позволяет злоумышленникам очень быстро масштабировать и изменять инфраструктуру.

Распространяемая таким образом вредоносная программа собирала существенную информацию об окружающей среде, в которой была запущена, на основании которой на следующем шаге скачивалась либо программа-вымогатель, либо программное обеспечение класса бэкдор.

Сопоставляя имеющиеся данные, специалисты ФинЦЕРТ пришли к заключению, что группа на самом деле не один раз атаковала российские финансовые организации. Ее атаки, еще не атрибутированные, отмечались и в течение 2020 года. Так, были выявлены рассылки от имени «Норильского никеля», «Финаудитсервиса», Российского союза промышленников и предпринимателей.

Начиная с августа способ распространения вредоносного программного обеспечения в выявленных фишинговых кампаниях изменился: теперь в сообщениях находилась короткая ссылка, сформированная через сервис bitly.com. По ссылке скачивался архив, содержащий утилиту wget, архиватор 7-Zip, TOR и первичный модуль, отвечающий за сбор информации об окружающей среде и дальнейшую загрузку необходимых по условиям модулей.

В результате анализа выявленных случаев были отмечены характерные для группы техники:

- использование обфусцированных сценариев JavaScript;
- применение обфусцированных сценариев PowerShell;
- внесение записи в раздел реестра Software\Microsoft\CurrentVersion\Run для закрепления бэкдора;
- сбор данных об окружении и пользователе;
- использование утилит для сбора информации о паролях;
- возможность установки иных модулей;
- использование workers.dev в качестве C2.

Группа умело применяет сочетание ВПО собственной разработки, продвинутых методов проникновения, а главное – социальной инженерии для успешного обмана сотрудников атакуемых организаций, в результате которого сотрудники совершают необходимые злоумышленникам действия.

Экспертными организациями, осуществляющими деятельность в сфере информационной безопасности, атаки данной группы также тщательно изучаются, и она уже получила условные названия, такие как TinyPosh или TinyScouts. Сообщается о применении злоумышленниками программ-шифровальщиков в отношении целей, не представляющих интерес с точки зрения развития атаки на инфраструктуру крупных организаций.

ФинЦЕРТ проверяет версию о причастности данной группы к совершению серии атак на поднадзорные Банку России организации еще в 2019 году с применением более простых, но в отдельных случаях весьма эффективных методов. Рассматривается вероятность иностранного происхождения группы с привлечением русскоговорящих участников. На данный момент информации о группе недостаточно, но есть вероятность, что ее атаки продолжатся в ближайшем будущем.

Вторая тенденция последних месяцев, на которую ФинЦЕРТ хотел бы обратить внимание, также представляется весьма опасной. Отдельные выявленные факты указывают на появление высококвалифицированной группы злоумышленников, занимающейся глубоким исследованием систем ДБО (в первую очередь мобильных приложений) с целью выявления уязвимостей, слабостей, особенностей клиент-серверного взаимодействия, которые позволяют получить не только персональные данные клиентов, но и в некоторых случаях – возможность хищения денежных средств.

Так, в I квартале 2020 года одной из российских экспертных организаций, работающих в сфере информационной безопасности, была опубликована информация о появлении в сети сервера, содержащего файлы с данными о клиентах одной из поднадзорных организаций:

- ФИО;
- пол;
- номер мобильного телефона;
- адрес электронной почты;
- место работы;
- номер счета;
- номер банковской карты с указанием срока действия;
- тип счета;
- валюта.

В совокупности в файлах было более 100 тыс. строк. Определить способ получения информации помогли находящиеся с файлами php-скрипты, предназначенные для эксплуатации выявленных уязвимостей при обращении с REST API мобильного приложения организации.

В результате расследования, проведенного самой поднадзорной организацией, было установлено, что злоумышленники эксплуатировали две уязвимости, которые носили программный характер и были связаны с механизмом авторизации при обращении к REST API. Это позволяло после прохождения процедуры аутентификации в системе получить доступ на просмотр данных другого клиента:

1. Номер счета, номер банковской карты с указанием срока действия, тип счета и указание валюты возвращались в результате эксплуатации уязвимости одного из ресурсов клиентского приложения, позволявшего использовать легитимные функции системы в нелегитимных целях. В данном случае в качестве параметра запроса передавался идентификатор операции (reference), выполненной клиентом. Идентификатор имеет следующую структуру (H03XXXXXXYYYYYYY):
   - H03 – код операции «Смена счета карты»;
   - XXXXXX – дата операции;
   - YYYYYYY – номер операции.

   В ответ на запрос в формате JSON возвращалась информация, содержащая сведения о смене привязки счета карты и включающая следующее:
   - дата выпуска карты;

- счет привязки;
- номер карты привязки;
- счет для привязки;
- срок действия карты;
- идентификатор клиента (CUS);
- прочая информация.

Путем перебора значений идентификатора операции (reference) злоумышленники получали доступ к данным об операциях других клиентов.

Для реализации данной схемы злоумышленниками использовался скрипт parse.php, найденный вместе с файлами на сервере. В нем были реализованы перебор идентификаторов операции, отсылка запросов, обработка и сохранение ответов в файл. Пример функции, формирующей запрос:

```
private function request( $reference = '' )
{
    $headers = [ 'Host: [redacted]',
                 'Accept: */*',
                 'Accept-Encoding: br, gzip, deflate',
                 'Accept-Language: ru',
                 'Content-Type: application/json',
                 'X-Request-ID: ' . $this->requestID,
                 'Origin: [redacted]',
                 'Content-Length: 0',
                 'Connection: keep-alive',
                 'X-CSRF-Token: ' . $this->csrfToken ];

    $ch = curl_init( '[redacted]' . $reference );

    curl_setopt( $ch, CURLOPT_HTTPHEADER, $headers );

    curl_setopt( $ch, CURLOPT_COOKIE, $this->cookie );

    curl_setopt( $ch, CURLOPT_USERAGENT, $this->userAgent );

    curl_setopt( $ch, CURLOPT_REFERER, '[redacted]' );

    curl_setopt( $ch, CURLOPT_POST, true );

    curl_setopt( $ch, CURLOPT_POSTFIELDS, '' );

    curl_setopt( $ch, CURLOPT_RETURNTRANSFER, true );

    curl_setopt( $ch, CURLOPT_SSL_VERIFYPEER, false );

    curl_setopt( $ch, CURLOPT_SSL_VERIFYHOST, false );

    $this->debug = "---Debug---<br />URL: [redacted][$reference]<br />cookie: {$this->cookie}<br />Headers: " . var_export( $headers, true );
```

2. ФИО, пол, номер мобильного телефона, адрес электронной почты и место работы возвращались в результате эксплуатации уязвимости другого ресурса клиентского приложения. В данном случае в качестве параметра запроса передается идентификатор клиента, например KYYYYY. В ответ приложение в формате JSON возвращает следующую информацию:
   - идентификатор клиента;
   - место работы, ФИО, номер телефона, прочая информация.

Путем перебора значений идентификатора клиента злоумышленники получали доступ к данным о клиентах. Для реализации этой схемы использовался скрипт next.php, найденный вместе с файлами на сервере, по набору реализованных функций и действий схожий с parse.php.

В другом известном ФинЦЕРТ случае итогом исследования злоумышленниками мобильного приложения поднадзорной организации и системы ДБО стало хищение денежных средств клиентов путем совершения операций без согласия с использованием в качестве транспорта платежной системы. Переводы были осуществлены двумя авторизованными клиентами поднадзорной организации через подмену номера счета отправителя на номер счета другого клиента банка (жертвы). Подмена произведена в сообщении, направленном из мобильного приложения в поднадзорную организацию после подтверждения платежа авторизованным клиентом. Указанные авторизованные клиенты организации в предыдущие дни провели успешную атаку по использованию недокументированной возможности API-интерфейса ДБО, в процессе которой смогли перебором получить номера счетов жертв.

Злоумышленники, используя режим отладки мобильного приложения, подменяют в исходящем на сервер ДБО сообщении о подтверждении платежа значение поля «Номер счета отправителя» на номер счета жертвы. При отправке сообщений на стороне сервера ДБО

не осуществлялась проверка принадлежности счета списания (поле «CustT_Contract_RID») авторизованному пользователю, что позволило злоумышленникам осуществить подмену.

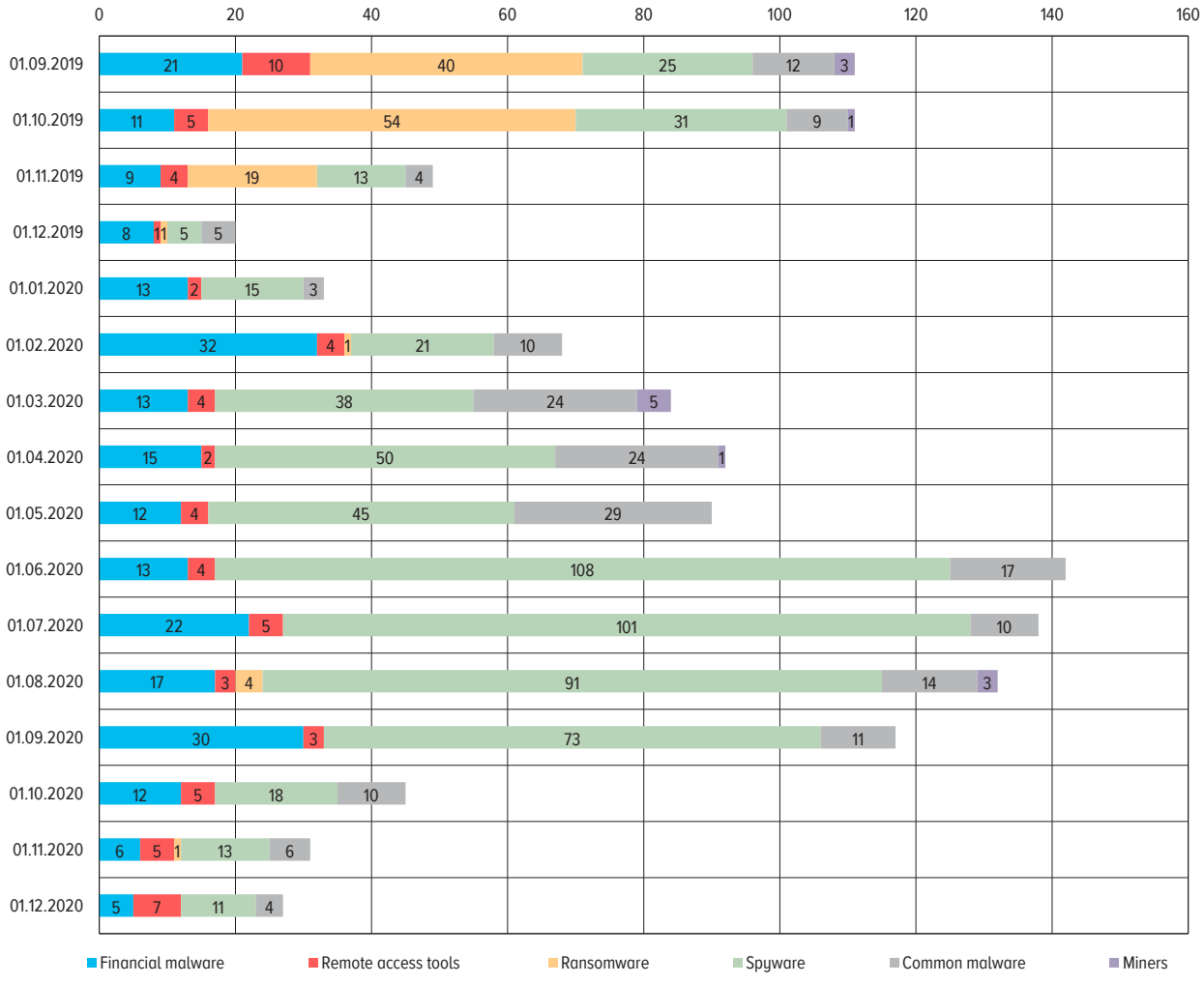
В ходе формирования распоряжения на перевод денежных средств СМС-сообщение с кодом подтверждения операции направлялось авторизованному пользователю. То есть все подтверждения злоумышленники осуществляли от лица своей легитимной учетной записи – клиента банка. Пострадавшие получали СМС-уведомления только по факту проведения операции после списания денежных средств со счета.

Данные инциденты показывают, что вектор внимания злоумышленников смещается с атак на непосредственную инфраструктуру кредитно-финансовых организаций на исследование клиент-серверных приложений с целью кражи данных клиентов или получения возможности хищения денежных средств со счетов клиентов.

Два приведенных примера не являются единственными случаями атак на мобильные приложения финансовых организаций, произошедшими за последнее время. ***ФинЦЕРТ настоятельно рекомендует организациям усилить меры, направленные на обеспечение защищенности мобильных компонент систем ДБО.***

Третья тенденция, отмеченная в 2020 году, – изменение состава ВПО, выявляемого участниками информационного обмена и направляемого в ФинЦЕРТ. Нагляднее всего тенденция может быть проиллюстрирована графически на примере последних 12 месяцев (рис. 25).

СОСТАВ РАССЫЛАЕМОГО ВПО ПО ДАННЫМ ИНФОРМАЦИОННОГО ОБМЕНА (ЕДИНИЦ) *Рис. 25*

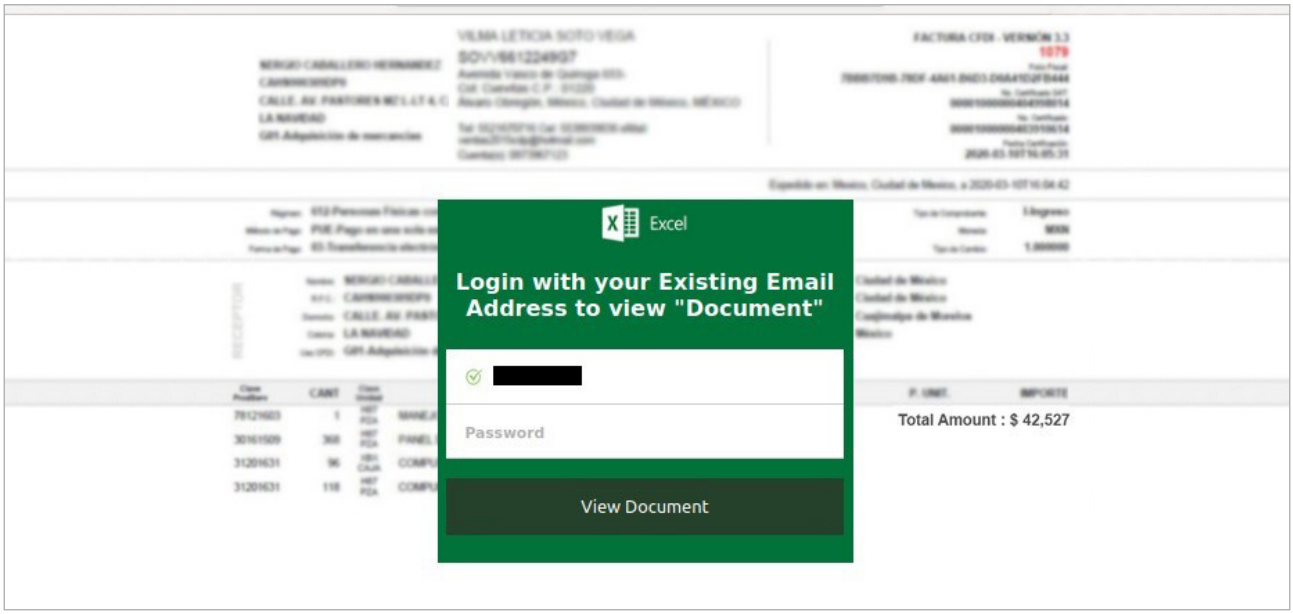


Поступление образцов программ-шифровальщиков в ФинЦЕРТ к концу 2019 года практически прекратилось, за исключением единичных случаев. Учитывая масштаб сети информационного обмена и разнообразие других источников, это не может быть случайным совпадением. По сообщениям экспертных организаций, количество распространяемых в мире программ-шифровальщиков, равно как и количество успешных атак, некоторые из которых были очень результативными в финансовом смысле, продолжает существенно увеличиваться. Очевидного и простого объяснения наблюдаемому явлению не имеется. Можно предполагать, что операторы программ-шифровальщиков, число которых, несмотря на большой резонанс от их распространения, является ограниченным, начали исключать финансовые организации из списков своих целей в связи с низкой результативностью.

На этом фоне впечатляет резкий рост количества разнообразных видов шпионского ВПО в потоке поступающих в ФинЦЕРТ образцов. Возросшее количество рассылок шпионского программного обеспечения нельзя отнести к появлению или активизации деятельности какой-либо конкретной группы. Вполне вероятно, что одновременно ими пользуются множество различных групп и одиночных злоумышленников. Наиболее активными в последнее время оказались Agent Tesla и его модификация Masslogger, LokiBot и Formbook. Резкое увеличение количества атак с применением шпионского ВПО имеет вполне объяснимые причины: криминальная индустрия нуждается в данных о клиентах финансовых организаций и о самих организациях для успешного использования в схемах атак с применением методов социальной инженерии. Списки клиентов с персональными данными – это самый популярный товар на криминальных ресурсах в течение последних полутора лет.

При этом нельзя сказать, что данные кампании ориентированы только на российские организации кредитно-финансовой сферы: текст и заголовки сообщений часто написаны на английском языке, используются не типичные для русскоязычных рассылок наименования компаний. Кроме того, в получателях среди российских организаций часто значатся те, кто имеет зарубежные филиалы или является дочерней компанией иностранной организации. Таким образом, усиленная охота за конфиденциальными данными ведется сегодня во всем мире.

На фоне роста рассылок шпионского программного обеспечения также отмечается рост рассылок, содержащих не исполняемые файлы, а скрипты, выводящие перед пользователем формы для ввода пароля от электронной почты под предлогом получения доступа к вложению, обновления данных, проверки безопасности. На экране компьютера пользователя срабатывание такого скрипта приводит к появлению формы ввода, как изображено на следующем рисунке.



Вводимый пользователем пароль отправляется по заранее вшитому в скрипт адресу, а перед пользователем выводится изображение или файл, не оказывающие какого-либо негативного влияния на рабочий компьютер пользователя. В некоторых случаях происходит проверка вводимого пароля и только при получении положительного ответа перед пользователем выводится изображение или файл, для получения доступа к которому требовался пароль.

На фоне существенных изменений в составе используемого для атак ВПО удивительную стабильность демонстрирует только группа RTM. На ее рассылки пандемия коронавирусной инфекции никак не повлияла – они продолжались весь год, за исключением небольшого перерыва в августе (пик сезона летних отпусков) и осенью – однако в этот период были отмечены аналогичные рассылки с ПО RMS. Более подробно о данной кампании рассказано в разделе «Атаки на информационную инфраструктуру клиентов организаций кредитно-финансовой сферы Российской Федерации».

Социальная инженерия в период пандемии

В условиях пандемии фиксируется значительный рост мобильного мошенничества, совершаемого в отношении граждан. Это связано с тем, что граждане, находясь в режиме самоизоляции, больше времени уделяют использованию мобильных телефонов (покупки, использование финансовых сервисов социальное общение и так далее).

Новая коронавирусная инфекция изменила не только уклад жизни населения Российской Федерации, но и переориентировала работу злоумышленников. Одним из популярных приемов в период пандемии стало использование таких тем, как компенсации, государственные пособия и государственная поддержка. Злоумышленники выманивали персональные данные и денежные средства у граждан под видом предоставления или помощи в получении мер государственной поддержки. Также активно появлялись сайты организаций без соответствующей лицензии, предлагающие гражданам легкий заработок на финансовом рынке.

Наиболее часто встречающимися направлениями фишинговых сайтов в этот период являлись интернет-магазины (48%) и социальные службы (43%). Это связано прежде всего с тем, что злоумышленники воспользовались введенными ограничениями и информацией о помощи, предоставляемой государством гражданам.

За период пандемии в рамках взаимодействия с регистраторами доменных имен снято с делегирования (перестали быть доступны для пользователей) 4314 сайтов мошеннического характера из 5011 направленных.

Анализ ситуации показал, что пик операций без согласия с точки зрения как объема сумм операций, так и общего их количества пришелся на конец марта – начало апреля. Это свидетельствует об использовании злоумышленниками сложившейся ситуации с пандемией для активизации противоправной деятельности с использованием ранее описанного инструментария (ВПО, фишинг, мошеннические звонки и СМС-рассылки).

Подобная активность злоумышленников привела к резкому росту объема и числа попыток операций без согласия клиента в период начала пандемии в среднем в два раза по сравнению с аналогичным периодом предыдущего года.

Спад активности злоумышленников в наблюдаемом периоде пришелся на май – до уровня +5% по количеству операций без согласия клиента и 50% по их объему по сравнению с показателями 2019 года, что в целом соответствует сезонным колебаниям в связи с майскими праздниками. При этом пандемия позволила злоумышленникам использовать как новые, так и старые способы вывода денежных средств.

Основные каналы вывода денежных средств:

1. Вывод через операторов электронных денежных средств системы (операторы ЭДС). Мошенники, вводя потерпевших в заблуждение, указывают номер виртуальной карты опера-

тора ЭДС, после получения денежных средств выводят их на обменники с целью сокрытия следов дальнейшего движения денежных средств.

2. Вывод на операторов сотовой связи. Мошенники осуществляют перевод денежных средств либо на баланс мобильного телефона с дальнейшим выводом денежных средств в сторону оператора ЭДС, либо указывают потерпевшему номер виртуальной карты, привязанной к счету мобильного телефона злоумышленника.
3. Переводы с карты на карту. Используя сервисы перевода денежных средств, мошенники, предварительно получив данные карты потерпевшего, осуществляют перевод денежных средств на заранее подготовленную «дроп»-карту.
4. Вывод на обменники (криптообменники). Одним из самых популярных выводов похищенных денежных средств является вывод на обменники, в том числе криптообменники. Обменники – сервисы, которые предоставляют возможность покупки/продажи валюты (криптовалюты), при которой сервис выступает в роли покупателя/продавца. Курс, по которому осуществляются обменные операции, выставляется непосредственно обменником. Как правило, курс на 5–10% выше рыночного. При этом отследить цепочку вывода денежных средств становится практически невозможно, так как переводы выполняются с разных счетов, заведенных в различных организациях кредитно-финансовой сферы.

ИНАЯ ДЕЯТЕЛЬНОСТЬ ФИНЦЕРТ В 2019–2020 ГОДАХ

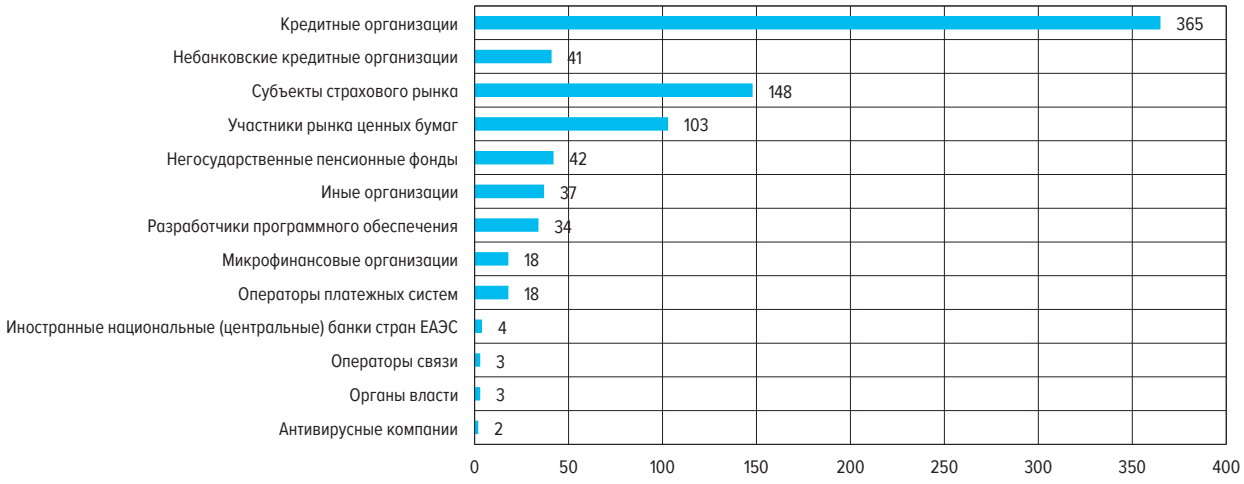
Информационный обмен: участники, инструменты, развитие

Участники информационного обмена

На протяжении всего периода деятельности ФинЦЕРТ развивает и расширяет сотрудничество с организациями, заинтересованными в обеспечении информационной безопасности, в том числе в кредитно-финансовой сфере. Так, в настоящее время к информационному обмену ФинЦЕРТ подключено 818 организаций. Стоит отметить, что участниками информационного обмена являются не только организации кредитно-финансовой сферы, но и компании-интеграторы, разработчики антивирусного программного обеспечения, иностранные финансовые организации и регуляторы, группы реагирования на инциденты (в том числе иностранные), провайдеры и операторы связи, государственные органы власти и иные организации.

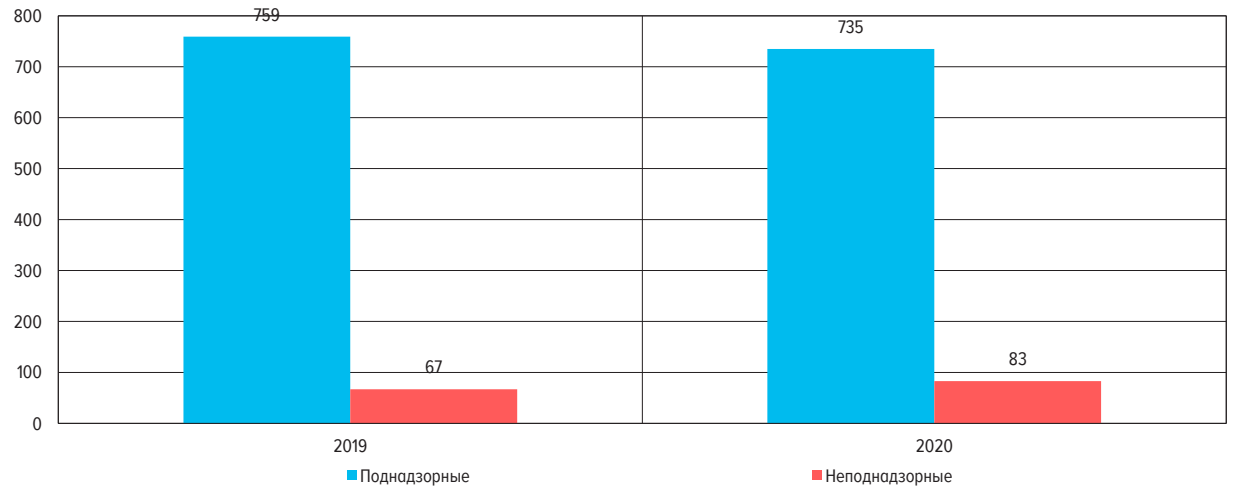
УЧАСТНИКИ ИНФОРМАЦИОННОГО ОБМЕНА
(ЕДИНИЦ)

Рис. 26



КОЛИЧЕСТВО УЧАСТНИКОВ
(ЕДИНИЦ)

Рис. 27



Изменение количества участников информационного обмена связано с ликвидацией (реорганизацией) юридических лиц, а также с механизмом и порядком отнесения некредитных финансовых организаций к подпадающим под критерии, предусмотренные Положением Банка России № 684-П.

Вместе с тем по сравнению с прошлым отчетным периодом количество неподнадзорных участников информационного обмена возросло на 16 организаций. Это может свидетельствовать о заинтересованности организаций из отличных от финансовой сферы областей деятельности в сотрудничестве с ФинЦЕРТ. Стоит отметить, что рассылаемая ФинЦЕРТ информация является актуальной не только для поднадзорных организаций.

Взаимодействие с вышеуказанными организациями осуществляется на безвозмездной основе на основании соглашений по вопросу противодействия компьютерным атакам.

При создании ФинЦЕРТ на первом месте стояла задача налаживания информационного обмена с организациями финансовой сферы Российской Федерации для информирования о наиболее актуальных и опасных компьютерных угрозах. Обмен данными осуществлялся посредством обмена электронными почтовыми сообщениями. Наиболее удобной формой обмена стали оперативные бюллетени в формате Adobe PDF, в которые включался типичный для CERT набор информации:

- краткое описание угрозы;
- имена файлов;
- хэш-суммы файлов (по алгоритмам SHA1, SHA256, MD5);
- размер файлов;
- сетевые индикаторы компрометации;
- данные о ресурсах электронной почты, используемой для распространения ВПО;
- заголовок и текст электронного сообщения;
- описание этапов атаки;
- рекомендации по противодействию.

Повсеместный рост автоматизации процессов мониторинга и реагирования на инциденты информационной безопасности поставил перед ФинЦЕРТ новую задачу: необходимость направления участникам информационного обмена информации об атаках также в машиночитаемом виде. В результате было принято решение использовать платформу с открытым исходным кодом для анализа угроз и обмена информацией MISP, которая уже применялась рядом зарубежных CERT и иных организаций в сфере информационной безопасности. MISP позволяет обеспечить совместное использование, хранение и корреляцию индикаторов компрометации целевых атак. Развитием платформы MISP в настоящее время занимается негосударственный CERT Люксембурга CIRCL.

С 2018 года участники информационного обмена стали получать от ФинЦЕРТ вместе с бюллетенями в формате Adobe PDF файлы в машиночитаемых форматах OpenIOC, STIX 1.0 и STIX 2.0, сформированные в MISP. Данные файлы содержали только индикаторы компрометации.

Направление информации в машиночитаемых форматах позволило ряду участников информационного обмена автоматизировать реагирование на поступающую от ФинЦЕРТ информацию по атакам. Однако в дальнейшем была выявлена проблема: машиночитаемые файлы в MISP формируются со специфической структурой, и во многих случаях это затрудняет их автоматическую обработку.

Кроме того, после ввода в 2018 году в эксплуатацию АСОИ ФинЦЕРТ произошло увеличение объема поступающей информации по различным атакам, однако оперативные бюллетени по-прежнему выпускались только по наиболее опасным из них. Большая часть информации при подобном подходе оставалась в распоряжении ФинЦЕРТ и использовалась только для статистического учета. Решением проблемы стал переход к регулярному направлению индикаторов компрометации по всем атакам, зафиксированным за сутки или несколько суток (если предыдущие дни были праздничными или выходными). Первоначально для рассылки был вы-

бран простой формат CSV (от англ. comma-separated values – «значения, разделенные запятыми»). В файле, размещаемом ежедневно в АСОИ ФинЦЕРТ, имеются следующие данные:

- дата поступления образца ВПО;
- название файла ВПО;
- хэш-суммы файлов по алгоритмам MD5, SHA-1 и SHA256;
- размер файла ВПО в байтах;
- данные о ресурсах, с которых осуществляется первоначальная загрузка ВПО;
- данные о ресурсах, с которыми ВПО осуществляет соединения, включая контрольно-командные сервера;
- данные о ресурсах электронной почты, через которую распространяется ВПО;
- класс ВПО по классификации, установленной для STIX2;
- семейство ВПО (наиболее распространенное наименование);
- источник информации о ВПО: информационный обмен ФинЦЕРТ, исследовательская организация, антивирусная компания.

В целях предоставления более структурированной информации, указания связей между индикаторами, предоставления контекста и источника идет проработка возможности дополнения ежедневных рассылок данными в формате STIX 2.x, состав данных и связи индикаторов в которых разрабатываются ФинЦЕРТ.

Система АСОИ ФинЦЕРТ

Для обеспечения процессов информационного обмена, а также повышения его оперативности и защищенности Банк России создал Автоматизированную систему обработки инцидентов (АСОИ ФинЦЕРТ). Применение АСОИ ФинЦЕРТ для информирования об инцидентах информационной безопасности предусмотрено Стандартом Банка России СТО БР БФБО 1.5–2018 «Безопасность финансовых (банковских) операций. Управление инцидентами информационной безопасности. О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации». Использование участником информационного обмена АСОИ ФинЦЕРТ позволяет существенно облегчить выполнение требований федеральных законов №187-ФЗ и №167-ФЗ, положений Банка России №382-П и №552-П и указаний Банка России №4926-У и №5039-У.

Создание АСОИ ФинЦЕРТ осуществлялось в два последовательных этапа: 2016–2018 годы (1-я очередь) и 2018–2020 годы (2-я очередь).

В 2018 году 1-я очередь АСОИ ФинЦЕРТ была протестирована кредитными организациями, успешно прошла приемочные испытания и приказом Банка России была введена в постоянную эксплуатацию.

В настоящее время[1] идет постоянное увеличение числа пользователей системы, а также расширение функционала АСОИ ФинЦЕРТ (завершаются работы по вводу в эксплуатацию АСОИ ФинЦЕРТ 2-ой очереди).

АСОИ ФинЦЕРТ построена на базе отказоустойчивой и защищенной инфраструктуры и состоит из информационного портала, сервиса личных кабинетов участников, специализированных технологических подсистем и подсистемы информационной безопасности. Функционал системы позволяет автоматизировать следующие процессы между участниками информационного обмена и ФинЦЕРТ:

- получение данных от участника (информация об инцидентах в организации, выявленных уязвимостях, угрозах, данных о раскрытии информации, запросах);

[1] *По состоянию на 31 декабря 2020 года.*

- передача участнику данных от ФинЦЕРТ об актуальных угрозах информационной безопасности в кредитно-финансовой сфере (в том числе из соответствующих бюллетеней ФинЦЕРТ);
- 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.

Реализация 2-ой очереди АСОИ ФинЦЕРТ расширяет возможности, предоставляемые участникам обмена с ФинЦЕРТ, а также позволяет оптимизировать взаимодействие с ФинЦЕРТ и перейти на автоматическое взаимодействие (без участия оператора в штатном режиме функционирования). В АСОИ ФинЦЕРТ 2-ой очереди присутствует следующий функционал:

- возможность передачи данных от участника в автоматическом режиме (по API) для всех видов инцидентов;
- расширены функции информационно-сервисного портала и сервисов личных кабинетов АСОИ ФинЦЕРТ;
- оптимизирована интерфейсная часть для повышения оперативности взаимодействия;
- реализован полнофункциональный тестовый контур АСОИ ФинЦЕРТ (зона опытной эксплуатации);
- в личном кабинете участника предоставляется сервис по проверке вредоносного программного обеспечения (включая отправку/получение информации по API и проверку вредоносных файлов в специализированной «песочнице»);
- дополнительные функции по проверке авторства и целостности сообщений/запросов при взаимодействии с участниками с использованием криптографических средств (сервис обмена электронными сообщениями между участниками и ФинЦЕРТ с использованием электронной подписи);
- возможность пошагового заполнения электронных форм при информировании об операциях, осуществленных без согласия клиента («визарды» для упрощения заполнения информации);
- реализация функционала распространения индикаторов компрометации (IOC, фидов) в машиночитаемых форматах бюллетеней для последующего их использования (в том числе в SIEM-системах участников);
- реализация функционала для участников по API-доступу к бюллетеням безопасности и соответствующим технологическим файлам, содержащим индикаторы компрометации (IOC);
- предоставление участникам возможности передачи через личный кабинет «дампов» сетевого трафика и лог-файлов web-серверов для последующего анализа в ФинЦЕРТ;
- предоставление сервиса уведомлений о критических инцидентах по SMS;
- предоставление сервиса автоматического и автоматизированного взаимодействия участников с ГосСОПКА (с получением соответствующих уведомлений о регистрации событий в ГосСОПКА);
- другие изменения, оптимизирующие решения, унаследованные из АСОИ ФинЦЕРТ 1-ой очереди.

В рамках работ по АСОИ 2-ой очереди проведены масштабирование и оптимизация решений, позволившие увеличить показатели назначения по объему обрабатываемой информации, а также по количеству участников обмена и одновременно работающим пользователям.

Текущая средняя нагрузка на АСОИ ФинЦЕРТ – до **1600** пользователей, одновременно работающих с системой, **более 5000** запросов в сутки, **до 250** публикаций бюллетеней и фидов по операциям без согласия клиентов в месяц.

С момента запуска АСОИ ФинЦЕРТ от участников получено и зарегистрировано свыше **3,2 млн** сообщений об инцидентах, из них более 80% – с использованием API для передачи информации в ФинЦЕРТ (в том числе по инцидентам, содержащим операции, осуществленные без согласия клиента).

Система «Фид-АнтиФрод»

В 2019 году на информационно-технологической базе АСОИ ФинЦЕРТ была введена в действие Автоматизированная система, реализующая формирование и ведение базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, – АС «Фид-АнтиФрод». АС «Фид-АнтиФрод» обеспечивает возможность выполнения Федерального закона № 167-ФЗ в части создания, формирования и ведения базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента и обеспечения возможности получения кредитными организациями данных из этой базы.

АС «Фид-АнтиФрод» предназначена для аккумулирования и быстрого обмена информацией об операциях без согласия клиента. Основными участниками такого обмена являются операторы по переводу электронных денежных средств, операторы услуг платежной инфраструктуры и Банк России. Информация об операциях без согласия клиента от участников информационного обмена передается в ФинЦЕРТ. Далее с использованием АС «Фид-АнтиФрод» и АСОИ ФинЦЕРТ осуществляется оперативное информирование кредитных организаций, являющихся получателями денежных средств по операциям, совершенным без согласия клиента. Затем в результате анализа информации по таким операциям формируются специальные сообщения для всех кредитных организаций (так называемые фиды, содержащие признаки операций, совершенных без согласия клиента), которые позволяют кредитным организациям применять меры как предупредительного характера, так и меры реагирования.

В результате функционирования АС «Фид-АнтиФрод» участники информационного обмена получают следующую информацию:

- хэшированные данные номеров паспортов, получателей денежных средств по операциям, осуществленным без согласия клиента;
- хэшированные данные СНИЛС, получателей денежных средств по операциям, осуществленным без согласия клиента;
- перечни ИНН организаций – получателей денежных средств по операциям, осуществленным без согласия клиента;
- перечни счетов получателей денежных средств и БИК банков по операциям, осуществленным без согласия клиента;
- перечни номеров карточек получателей денежных средств по операциям, осуществленным без согласия клиента;
- перечни номеров телефонов получателей денежных средств, задействованных в операциях, осуществленных без согласия клиента;
- перечни номеров электронных кошельков получателей денежных средств, задействованных в операциях, осуществленных без согласия клиента.

По состоянию на декабрь 2020 года накоплено более 43 тыс. уникальных признаков операций, совершенных без согласия клиента, в том числе 23 444 карт, 12 637 хэшей паспортов, 4 723 телефонов, 1 237 счетов, 1 100 электронных кошельков, 266 ИНН.

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

После завершения работ по вводу в эксплуатацию АСОИ ФинЦЕРТ 2-ой очереди планируется инициация работ по дальнейшему развитию АСОИ ФинЦЕРТ и АС «Фид-АнтиФрод».

Применение АСОИ ФинЦЕРТ участниками обмена

Основным способом взаимодействия с участниками информационного обмена является инфообмен с использованием АСОИ ФинЦЕРТ. В случае недоступности основного канала используются резервные способы (электронная почта и телефон дежурной службы ФинЦЕРТ).

Каждый участник информационного обмена получает доступ в личный кабинет АСОИ ФинЦЕРТ. При этом подключение участников, поднадзорных Банку России, осуществляется на основании заполненной и направленной на электронную почту (info_fincert@cbr.ru) карточки участника информационного обмена, для неподнадзорных – на основании заключенного соглашения (типовая форма размещена на официальном сайте Банка России в разделе «Информационная безопасность/ФинЦЕРТ») и предоставленной карточки участника информационного обмена.

На инфопортале АСОИ ФинЦЕРТ, доступном всем участникам обмена, размещается вся необходимая информация:

- текущий режим функционирования и информация о плановых работах в АСОИ ФинЦЕРТ и АС «Фид-АнтиФрод»;
- документация на системы в части передаваемой участникам обмена и разработчикам;
- информация по использованию API;
- порядок подключения и использования системы;
- дополнительное программное обеспечение (в случае его использования участником и т.д.);
- часто задаваемые вопросы/ответы (FAQ) и другая справочная информация.

АСОИ ФинЦЕРТ поддерживает получение и прием информации от участников инфообмена, передаваемой путем:

- заполнения в личном кабинете интерактивных форм об инцидентах, уязвимостях, угрозах, операциях, осуществленных без согласия клиентов, и т.д.;
- заполнения в личном кабинете информации по инцидентам с использованием заранее приготовленных соответствующих сообщений-шаблонов (прикрепление json-файлов сообщений об инцидентах);
- передачи информации, предусмотренной Стандартом Банка России СТО БР БФБО-1.5–2018 «Безопасность финансовых (банковских) операций. Управление инцидентами информационной безопасности. О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации» в виде json-файлов, оформленных в соответствии с форматами системы и загружаемых в личный кабинет оператором участника;
- взаимодействия систем на стороне участников обмена с АСОИ ФинЦЕРТ по API (прикладному протоколу программного взаимодействия) при непосредственном формировании сообщений на стороне участника;
- взаимодействия систем на стороне участников обмена с АСОИ ФинЦЕРТ по API (прикладному протоколу программного взаимодействия) при использовании унифицированных механизмов взаимосвязи SIEM систем (по протоколу syslog) и специализированной компоненты, устанавливаемой на стороне участника и обеспечивающей отправку сообщений установленного формата в ФинЦЕРТ;
- передачи файлов для проведения анализа на наличие вредоносного программного обеспечения (как интерактивно, так и с использованием API).

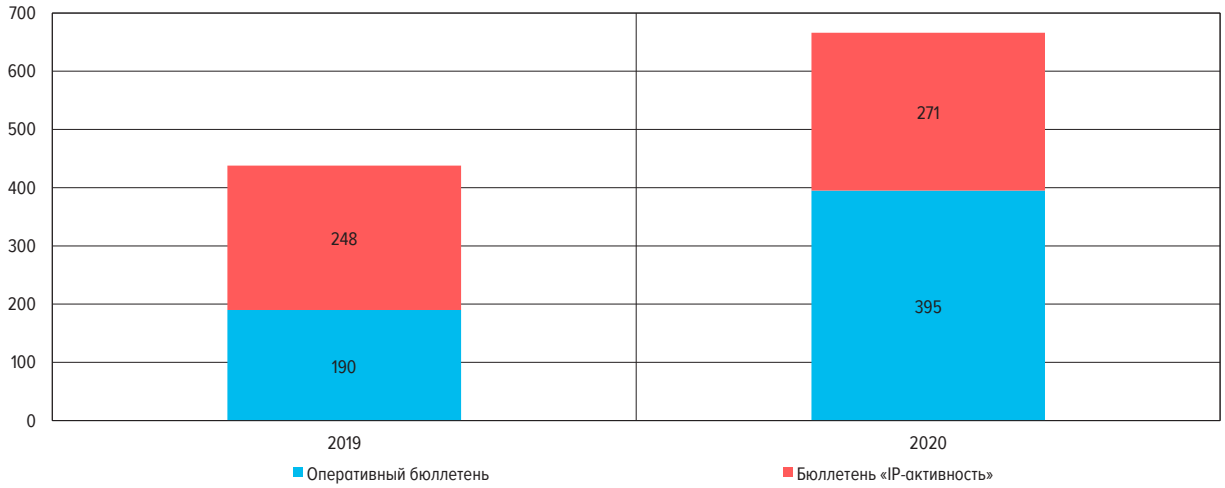
Информирование участников

ФинЦЕРТ на регулярной основе выпускает бюллетени по информационной безопасности. Данные бюллетени содержат индикаторы компрометации, а также рекомендации по минимизации возможных негативных последствий и принятию превентивных мер реагирования.

За 2020 год ФинЦЕРТ направил 395 оперативных бюллетеней, а также 271 бюллетень по IP-активности, по сравнению с прошлым годом количество бюллетеней увеличилось на 52%. Это изменение связано прежде всего с трансформацией вектора компьютерной атаки в период коронавирусной инфекции, а также перемещением фокуса внимания злоумышленников на граждан.

ВИДЫ РАССЫЛАЕМЫХ БЮЛЛЕТЕНЕЙ ФИНЦЕРТ
(ЕДИНИЦ)

Рис. 28



Также ФинЦЕРТ оказывает практическую и информационную помощь в режиме 24/7 по реагированию на компьютерные инциденты. Так, ФинЦЕРТ направляет информацию о сайтах и номерах телефонов, которые использовались в недобросовестных целях в кредитно-финансовой сфере, в адрес уполномоченных организаций, консультирует по вопросу информирования Банка России о компьютерных инцидентах, оказывает содействие в реагировании на инциденты, предоставляя организациям рекомендации.

Оказываемая помощь и рассылаемые бюллетени позволяют минимизировать риски наступления негативных последствий компьютерных атак и инцидентов, принять превентивные меры и подготовить инфраструктуру организаций к возможным угрозам.

Международное сотрудничество

В текущем отчетном периоде деятельность ФинЦЕРТ по международному сотрудничеству развивалась по двум направлениям – интеграционному и двустороннему.

В рамках сотрудничества с центральными (национальными) банками стран – участниц ЕАЭС по вопросу противодействия компьютерным атакам реализован обмен информацией о киберугрозах через АСОИ ФинЦЕРТ. В текущем отчетном периоде от центральных (национальных) банков стран ЕАЭС было получено 173 сообщения по вопросам информационной безопасности, направлено более 400 бюллетеней. Также запланировано проведение стажировки с целью обмена опытом и лучшими практиками по вопросам информационной безопасности.

Развивается сотрудничество в рамках площадки БРИКС в области обеспечения информационной безопасности. Была организована совместная трехсторонняя встреча представителей Банка России, Центрального банка Бразилии и Резервного банка Индии в рамках XII Уральского форума «Информационная безопасность финансовой сферы», который прошел с 17 по 21 февраля 2020 года в Республике Башкортостан.

В рамках двустороннего сотрудничества подписано соглашение о взаимодействии между Центральным банком Российской Федерации и Центральным банком Республики Узбекистан по вопросу противодействия компьютерным атакам. Также налаживается сотрудничество по данному направлению с Национальным банком Республики Таджикистан и Центральным банком Республики Туркменистан, а также с центральными банками Италии, Испании и Индонезии.

Сотрудничество с вышеуказанными странами и интеграционными объединениями позволит обмениваться опытом и лучшими практиками по вопросу противодействия компьютерным атакам, принимать превентивные меры и минимизировать негативные последствия.

Также в рамках международного сотрудничества при выявлении компьютерной атаки ФинЦЕРТ уведомляет об этом иностранные центральные банки с целью принятия ими мер реагирования, а также минимизации риска наступления негативных последствий. Так, за отчетный период ФинЦЕРТ уведомил иностранные центральные банки более 30 стран, в числе которых Германия, Швейцария, Франция, Португалия и другие. Иностранные партнеры положительно отозвались о рассылаемой информации и приняли ее в работу.

Повышение киберграмотности населения

В 2020 году интерес общественности к теме мошенничества с помощью приемов и методов социальной инженерии и хищений средств с использованием ЭСП вырос в 1,6 раза. Число сообщений в СМИ по этой теме составило 83 022 против 51 550 годом ранее. Пропорционально увеличилось число сообщений по теме телефонного мошенничества: 22 200 против 13 869 сообщений. Это свидетельствует об общественной потребности в информации на указанную тему.

Рост ее актуальности в общественной повестке коррелирует с ростом активности злоумышленников, о которой говорилось ранее. При этом рост объема хищений и снижение объема возмещения в 2020 году[2] свидетельствуют о том, что устойчивость граждан к используемым злоумышленниками приемам и методам социальной инженерии, несмотря на снижение доли совершенных с ее помощью операций без согласия клиентов, остается по-прежнему на низком уровне.

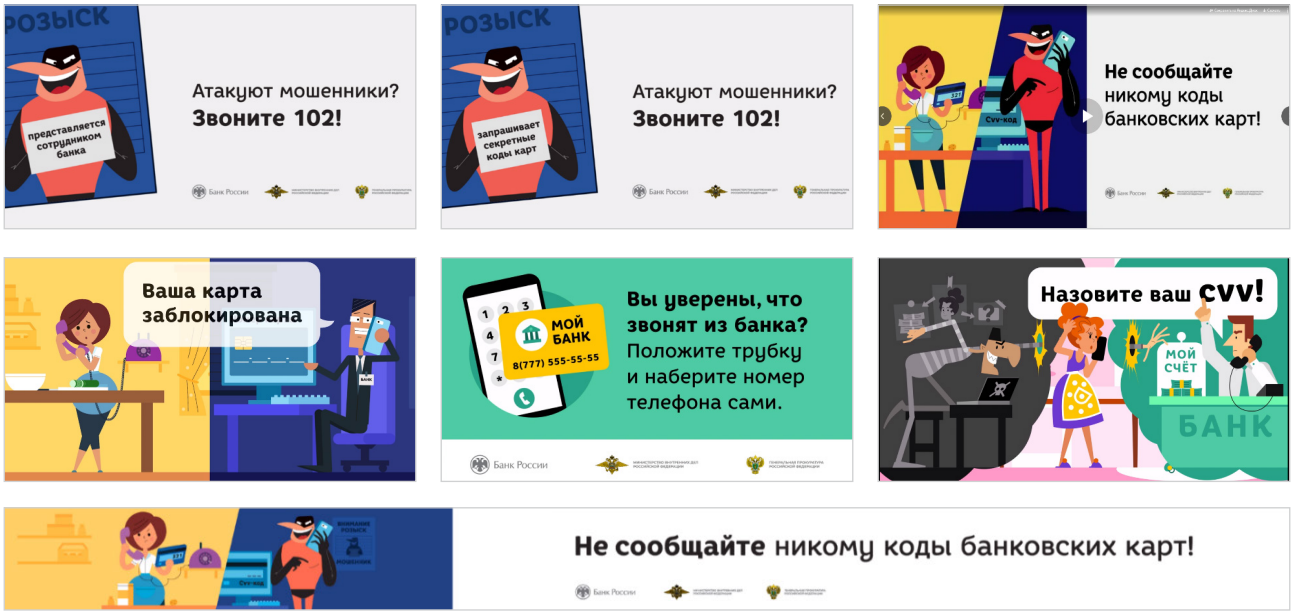
Противодействие операциям без согласия клиента на финансовом рынке путем повышения цифровой культуры и киберграмотности – одно из направлений деятельности Банка России. Для максимального охвата аудитории целевых социальных и возрастных групп Департамент по связям с общественностью (ДСО) совместно с Департаментом информационной безопасности (ДИБ) и Службой по защите прав потребителей и обеспечению доступности финансовых услуг используют разнообразные современные каналы и форматы взаимодействия.

На сайте *«Финансовая культура»* в разделе «Осторожно: мошенники!» размещены материалы, в доступной форме информирующие о том, как защитить свои средства от финансовых мошенников, распознать злоумышленника по телефону, определить фишинговое письмо или сайт. В разделе «Грабли» разбираются реальные ситуации и даются практические советы гражданам, как не попасть в сети мошенников.

Тема противодействия мошенничеству освещается и на страницах Банка России в социальных сетях. Наиболее популярными и дающими широкий охват аудитории стали креативные материалы в специальных форматах – карточки, тесты. Среди самых заметных – «Новогодние мошенники» (3,509 млн просмотров), «Как защитить детей от онлайн-мошенников» (581,8 тыс.), «Фантастические мошенники и как с ними бороться» (более 250 тыс.), «Мошенники и коронавирус» (476,6 тыс.). Использование рекламного инструментария для самых значимых и интересных публикаций расширяет охват аудитории за пределы подписчиков страниц. Кроме подключения прямого рекламного продвижения, некоторые материалы распространяются через тематические паблики и сообщества в социальных сетях.

Еще одним вектором работы с темой является сотрудничество с лидерами мнений, блогерами. Интеграция в каналы блогеров происходит максимально нативно (естественно для аудитории), без использования бренда Банка России. В декабре 2019 года и апреле 2020 года

[2] *Соответствующие данные будут опубликованы в Отчете об операциях без согласия клиентов финансовых организаций за 2020 год.*



были проведены две информационные кампании с интеграцией в каналы блогеров. Их целью было проинформировать аудиторию о типичных приемах мошенников (социальная инженерия – телефонные звонки из службы безопасности банка и другие уловки). Охват декабрьской кампании составил почти 120 тыс. просмотров, апрельской – более 196 тыс. просмотров. Пользователи активно вовлекались в дискуссии и делились в комментариях своими историями – было опубликовано более 1000 комментариев.

В целях информирования более широкой аудитории о том, как противостоять разного рода финансовым мошенничествам, Банк России реализует партнерские программы. Совместно с МВД России и органами Прокуратуры Банк России проводит информационную кампанию по тематике противодействия операциям без согласия клиента. Материалы социальной рекламы регулярно размещаются на билбордах и объектах транспортной инфраструктуры Москвы и ряда субъектов Российской Федерации.

В 2020 году проведено более 20 публичных информационно-обучающих мероприятий для разных целевых аудиторий. Примерная численность прошедших обучение, а также слушателей по всем мероприятиям составила более 200 тыс. человек.

Сотрудники ДИБ активно участвуют в онлайн-уроках, организуемых Банком России. С учетом перевода школьников на дистанционный режим обучения в период пандемии онлайн-уроки стали еще более востребованными. Обеспечена разработка учебно-методических комплексов для учебных заведений высшего и среднего образования по тематике информационной безопасности, а также проведение кибердиктанта.

ПРИЛОЖЕНИЕ

Рекомендации по предотвращению компьютерных атак и действиям в случае успешной реализации атак

Как мы уже отмечали ранее, значительно возросло число атак с применением различного шпионского программного обеспечения. Основными мерами противодействия подобным атакам являются организационные, такие как повышение осведомленности сотрудников в области информационной безопасности и проведение тренировок сотрудников (например, рассылка тестовых фишинговых писем, анализ успешных проникновений) с обязательным подведением итогов тренировок.

При этом не стоит забывать про соблюдение ряда технических мер:

- использование антивирусного программного обеспечения на компьютерах пользователей и серверах, а также своевременное обновление его баз;
- регулярный мониторинг и установка исправлений (патчей) безопасности распространенного офисного программного обеспечения и операционных систем;
- периодическая проверка на индикаторы компрометации, получаемые как в результате обмена с ФинЦЕРТ и другими участниками рынка, так и из открытых источников;
- регулярное обновление сигнатур для систем IDS/IPS и подписок Threat Intelligence для своевременного детектирования подозрительного трафика и поведения;
- установка на банкоматы и платежные терминалы программного обеспечения контроля целостности и предотвращения несанкционированного запуска сторонних программ;
- своевременный вывод из эксплуатации неподдерживаемого производителем программного обеспечения в случае наличия такой возможности;
- проведение политики ограничения использования учетных записей с повышенными привилегиями, ограничение количества учетных записей локальных администраторов;
- исключение использования сотрудниками паролей, не соответствующих требованиям безопасности;
- исключение хранения в открытом виде паролей доступа к критичным для организации информационным системам;
- проведение регулярных тренингов с сотрудниками организации по линии осведомленности в области информационной безопасности, а также организация периодических учений для проверки устойчивости к атакам с использованием социальной инженерии;
- проведение полноценных киберучений для проверки готовности профильных подразделений противостоять атакам на информационную инфраструктуру организации;
- исключение возможности неконтролируемого доступа в сеть Интернет в обход межсетевых экранов и иных программно-аппаратных средств.

Для улучшения процессов обнаружения и реагирования на атаки необходимо:

- вести протоколы (журналы, логи) сетевых соединений пограничного с сетью Интернет устройства, установить достаточный период их хранения для возможного расследования инцидентов информационной безопасности;
- обеспечить контроль за установленным на компьютерах пользователей и серверах программным обеспечением – возможно, с помощью реализации технологии «белых списков»;
- проводить политику ограничения массового использования средств удаленного администрирования, особенно на участках платежной системы Банка России;

- обеспечить протоколирование и хранение журналов сеансов администрирования для средств удаленного администрирования, ограничить диапазон IP-адресов, с которых возможно удаленное подключение;
- обеспечить контроль и логирование доступа пользователей к критичным для организации информационным системам.

При этом организациям стоит уделять особое внимание атакам, ориентированным на клиентов – юридических лиц, поскольку именно эти атаки сейчас наиболее активны и несут наибольший ущерб.

Меры противодействия подобным атакам со стороны организации кредитно-финансовой сферы:

- настройка правил антифрода, учитывающих типовые платежи клиента, а также оповещение клиента при срабатывании подобных правил;
- оповещение всех клиентов об актуальных способах хищений с указанием возможных мер противодействия со стороны клиента;
- проведение регулярных тренингов с представителями организаций-клиентов по линии осведомленности в области информационной безопасности.

Меры противодействия со стороны клиента:

- использование антивирусного программного обеспечения, а также своевременное обновление его баз;
- регулярное полное сканирование информационных систем средствами антивирусной защиты;
- выполнение всех рекомендаций по работе с вложениями, пришедшими из подозрительных источников, в том числе рекомендаций не открывать вложения – исполняемые файлы и не включать макросы в документах Microsoft Office, если нет уверенности в надежности отправителя;
- постоянная визуальная проверка в системе ДБО всех реквизитов платежных поручений;
- отказ в подтверждении вызывающих сомнение платежей до выяснения всех обстоятельств.

Рекомендации для граждан по противодействию атакам с применением методов социальной инженерии

С целью повышения уровня безопасности граждан ФинЦЕРТ проводит мероприятия по киберграмотности, в рамках которых предоставляются рекомендации по превентивным мерам противодействия хищению денежных средств.

Для того чтобы обезопасить себя, гражданам следует запомнить несколько простых правил:

1. Не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам. Даже если ссылка кажется надежной, а телефон верным, всегда сверяйте адреса с доменными именами официальных сайтов организаций, а номера проверяйте в официальных справочниках. Официальные адреса кредитных организаций указаны в перечне web-адресов кредитных организаций, размещенном *на официальном сайте Банка России*.
2. Если вам приходит СМС о зачислении средств (и сообщение похоже на привычное уведомление банка), а затем звонит якобы растяпа, который по ошибке зачислил вам деньги и просит вернуть, не спешите их переводить. Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не приходили, СМС – не от вашего банка, а звонил вам злоумышленник. Проверьте состояние вашего счета, закажите выписку в онлайн-банке, позвоните в банк, прежде чем переводить кому-то деньги.
3. Если вам приходит уведомление «Подтвердите покупку» и код, а следом раздается звонок опять же от «рассеянного» человека, который говорит, что по ошибке указал ваш телефонный номер, и просит продиктовать ему код, ни в коем случае не делайте этого. Мошенни-

ки пытаются выманить у вас код, чтобы списать с вашего счета средства или подписать вас на ненужный платный сервис.

4. Никому не сообщайте персональные данные, а уж тем более пароли и коды. Сотрудникам банка они не нужны, а мошенникам откроют доступ к вашим средствам.
5. Не храните данные карт на компьютере или в смартфоне.
6. Проверяйте информацию. Если вам говорят, будто вы что-то выиграли или с вашей карты случайно списали деньги и нужно назвать свои данные, чтобы остановить операцию, закончите разговор и перезвоните в банк по номеру телефона, указанному на обратной стороне карты или на официальном сайте банка.
7. Если вам сообщают, что у родственников или друзей неприятности, постарайтесь связаться с ними напрямую.
8. Установите и обязательно обновляйте антивирусные программы на всех используемых устройствах – и себе, и родственникам.
9. Если вам поступает звонок якобы от службы безопасности банка, в котором вы обслуживаетесь, с информацией о том, что кто-то пытается с использованием ваших персональных данных взять кредит или осуществить несанкционированную операцию с вашего счета, не спешите следовать инструкциям злоумышленника. Положите трубку, перезвоните в банк по номеру телефона, указанному на банковской карте или на официальном сайте организации, и уточните полученную информацию.