ОБЗОР ОСНОВНЫХ ТИПОВ КОМПЬЮТЕРНЫХ АТАК В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ В 2018 ГОДУ

БАНК РОССИИ
ФИНЦЕРТ

СОДЕРЖАНИЕ

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

Фото на обложке: Shutterstock.com

107016, Москва, ул. Неглинная, 12
Официальный сайт Банка России: www.cbr.ru

Список сокращений

АСОИ ФинЦЕРТ	Автоматизированная система обработки инцидентов
АС «Фид-Антифрод»	Автоматизированная система «Фид-Антифрод»
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
Методы атаки	Совокупность приемов, которые использовались злоумышленниками для достижения цели
Положение Банка России № 382-П	Положение Банка России от 9.06.2012 №382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»
Программа-шифровальщик	Вредоносная компьютерная программа, осуществляющая скрытое шифрование компьютерной информации пользователя с последующим вымогательством денежных средств за расшифровку
Спуфинг	Подмена в электронном почтовом сообщении видимого адреса отправителя для обмана получателя
Фишинг	Вид мошенничества в сети Интернет, целью которого является получение каких-либо конфиденциальных данных пользователей
Хакинг	Эксплуатация уязвимостей в доступных для подключения сетевых службах. Подбор учетных данных и использование уязвимостей веб-приложений выделены в отдельные категории для большей детализации
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
Spear-phishing	Целевой фишинг с использованием приемов социальной инженерии или какой-либо заранее известной атакующему информации о цели

ВВЕДЕНИЕ

Одной из важнейших задач Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Банка России является анализ данных о компьютерных атаках на организации кредитно-финансовой сферы и их клиентов.

В настоящем обзоре приводятся сведения об основных типах компьютерных атак, зафиксированных ФинЦЕРТ, а также рядом компаний – участников рынка информационной безопасности в 2018 году. Дополнение ежегодно выпускаемого ФинЦЕРТ обзора основных видов атак данными независимых аналитиков, участвующих в информационном обмене ФинЦЕРТ, позволяет сформировать максимально объективную и полную картину ландшафта киберрисков кредитных и некредитных финансовых организаций. Представленные в разделе «Заключение» выводы сделаны на основе консолидированного мнения всех авторов обзора.

В целом, подводя итоги анализа основных типов компьютерных атак и их параметров за 2018 г., авторы отмечают серьезное значение для получения четкой картины криминальных угроз полноты и качества сведений, передаваемых участниками информационного обмена в том числе через АСОИ ФинЦЕРТ. Ответственное отношение участников к исполнению установленных требований по информированию позволит получить по итогам 2019 г. наиболее точную картину компьютерной преступности в кредитно-финансовой сфере за все время проведения таких исследований в нашей стране. Ввиду того, что ближайшем будущем не следует ожидать существенного снижения количества и опасности компьютерных атак в кредитно-финансовой сфере, использование материалов обзора в практике обеспечения информационной безопасности финансовых организаций способствует минимизации рисков реализации киберугроз в данной сфере.

Информация из обзора может быть использована руководителями и специалистами в целях планирования мероприятий по информационной безопасности и для ознакомления персонала с основными видами актуальных угроз.

ФИНЦЕРТ: ОСНОВНЫЕ ТИПЫ АТАК НА ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ ОРГАНИЗАЦИЙ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕТОДОЛОГИЯ

Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Банка России был создан в 2015 г. с целью консолидации участников финансового рынка и рынка информационной безопасности в борьбе против компьютерной преступности. Основной задачей ФинЦЕРТ является организация обмена информацией, что позволяет оперативно реагировать на возникающие угрозы в области информационной безопасности.

Подключение к информационному обмену дает каждому участнику право в любой момент времени обращаться за помощью специалистов ФинЦЕРТ в случаях обнаружения вредоносного программного обеспечения в информационной системе, выявления попыток эксплуатации уязвимостей программного обеспечения, подозрительных сетевых взаимодействий и в целом в любых случаях иных компьютерных атак. Предоставление информации об атаках в ФинЦЕРТ необходимо как для оказания непосредственной помощи выявившим их участникам, так и для предупреждения при необходимости остальных участников информационного обмена.

Важным источником сведений о компьютерных атаках является также участие специалистов ФинЦЕРТ в проведении криминалистических исследований образцов вредоносного программного обеспечения (ВПО), а также носителей информации, подвергшихся воздействию ВПО или других компьютерных атак. Исследования проводятся на основании официальных обращений об оказании помощи участников информационного обмена и запросов правоохранительных органов. Кроме того, специалисты ФинЦЕРТ периодически выезжают в организации, пострадавшие от компьютерных атак, для оказания на месте помощи по ликвидации их последствий, выявлению всех обстоятельств атак и пострадавших средств вычислительной техники, сбора и фиксации цифровых следов атак для последующего обращения в правоохранительные органы и экспертные организации.

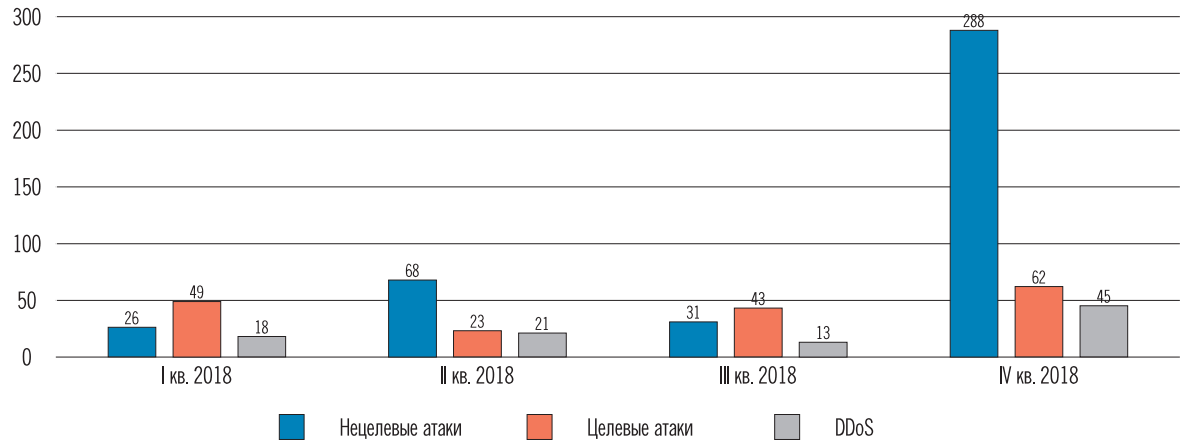
В комплексе вся указанная деятельность позволяет ФинЦЕРТ изучать механизмы компьютерных атак в кредитно-финансовой сфере (КФС), поддерживать максимально полное представление Банка России о компьютерной преступности, необходимое для разработки и актуализации законодательства, регулирующего вопросы обеспечения информационной безопасности финансовых организаций.

АСОИ ФинЦЕРТ

С июля 2018 г. введена в эксплуатацию автоматизированная система обработки инцидентов ФинЦЕРТ (АСОИ ФинЦЕРТ), с использованием которой осуществляется передача информации об атаках от участников, ведется взаимодействие со специалистами ФинЦЕРТ, производится рассылка оперативных бюллетеней с указанием основных индикаторов компрометации и рекомендациями по предотвращению проникновения ВПО. Данная система уже сейчас позволяет получать больше сведений о компьютерных атаках и распространении вредоносного программного обеспечения и, таким образом, составлять более полную картину действий компьютерной преступности в отношении организаций кредитно-финансовой сферы России. Необходимо отметить, что скачки в статистических данных за 2018 г., приходящиеся на IV квартал, в первую очередь связаны именно с введением в строй АСОИ ФинЦЕРТ.

Всего за год ФинЦЕРТ получены сведения о 687 атаках, в том числе о 177 целевых[1] атаках, осуществленных на кредитно-финансовые организации в 2018 году.

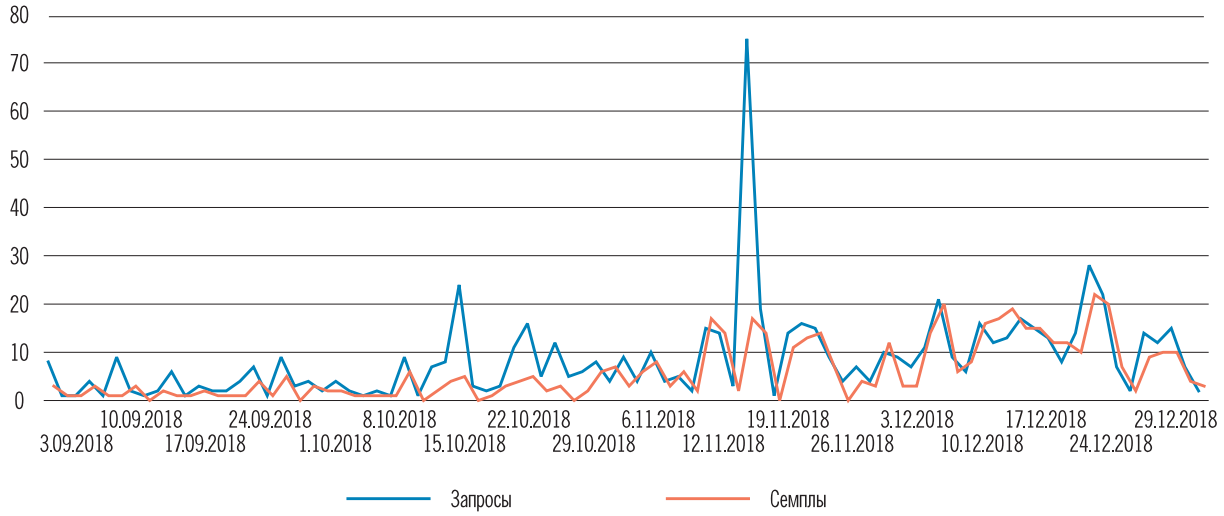
Полученные ФинЦЕРТ сведения об атаках за 2018 год



В период с сентября по декабрь 2018 г. через АСОИ ФинЦЕРТ от участников информационного обмена было получено 727 обращений, содержащих 506 образцов ВПО.

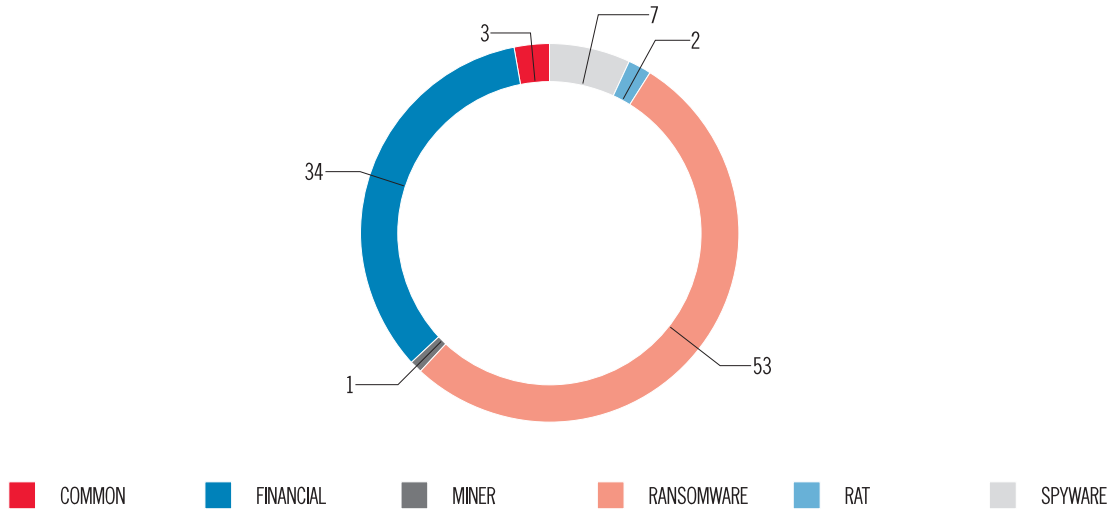
[1] *В контексте настоящей статистики под целевыми атаками специалистами ФинЦЕРТ подразумеваются атаки, направленные на получение финансовой выгоды и затрагивающие организации кредитно-финансовой сферы.*

Отношение общего количества запросов, полученных через АСОИ за сентябрь-декабрь 2018 г., к количеству запросов, содержавших образцы ВПО



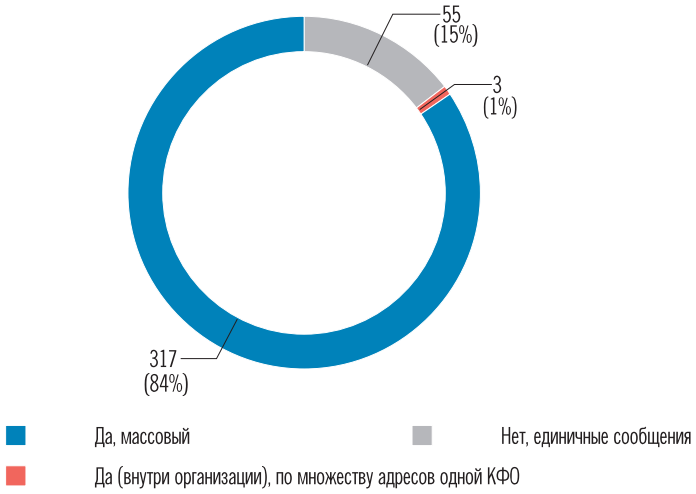
Рассылками ВПО, зафиксированными в указанный выше период, преимущественно распространялось ВПО класса ransomware (программы-вымогатели, шифровальщики) и так называемое финансовое ВПО, конечной целью использования которого является хищение денежных средств (53 и 34% рассылок соответственно).

Распределение зафиксированных кампаний распространения ВПО в сентябре-декабре 2018 г. по классам



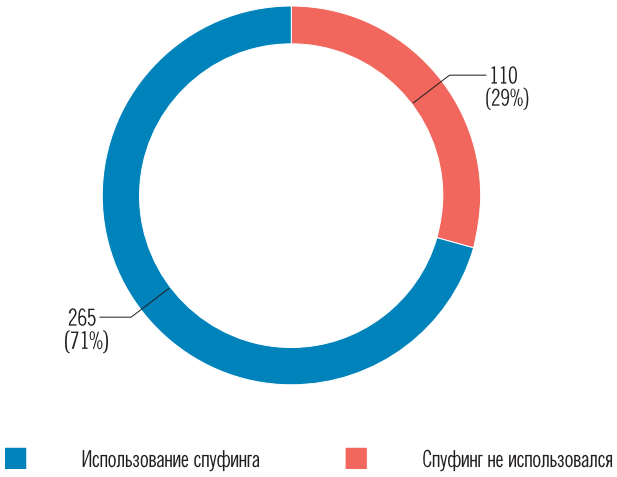
В этот период было зафиксировано 375 отдельных кампаний по распространению ВПО, из них 317 имели массовый характер.

Характер зафиксированных рассылок ВПО



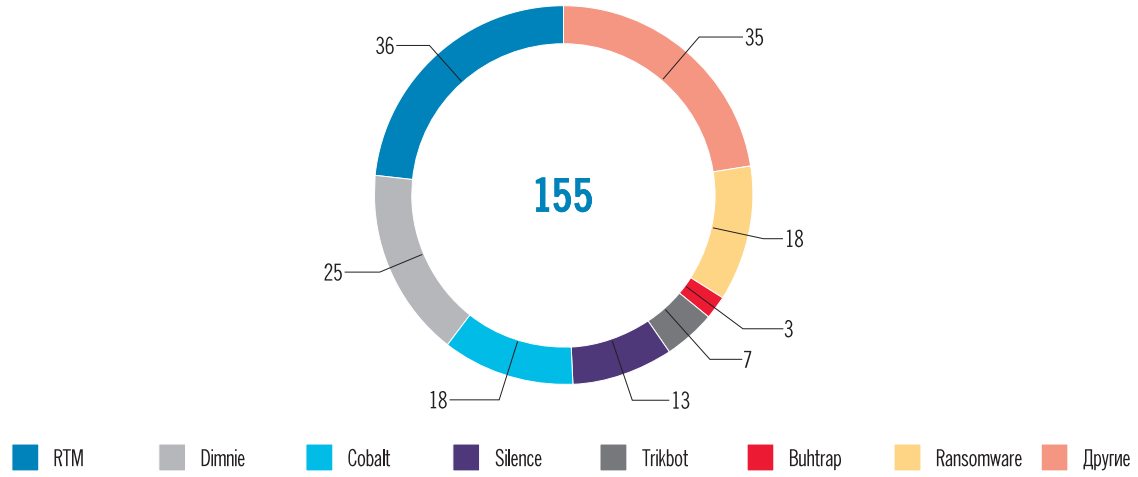
В 265 случаях для рассылки ВПО применялся спуфинг (подмена) электронных почтовых адресов.

Отношение числа кампаний с использованием спуфинга адресов к числу прочих



За 2018 г. специалистами ФинЦЕРТ было выпущено 155 оперативных бюллетеней с индикаторами компрометации систем и сетей по фактам наиболее опасных кампаний по распространению ВПО. Это значительно больше, чем в 2017 г., когда было выпущено 48 таких бюллетеней (не считая бюллетеней с обновлениями/дополнениями и кратких оповещений по электронной почте). Рост количества выпущенных предупреждений стал возможен в том числе благодаря введению в строй АСОИ ФинЦЕРТ.

Количество выпущенных бюллетеней с распределением по типу угрозы



Также отметим, что в 2018 г. суммарно было выявлено более 540 ресурсов в сети Интернет, распространяющих ВПО или являющихся управляющими серверами ВПО. При этом более 500 из этих ресурсов зарегистрировано за пределами Российской Федерации. Расположение подобных ресурсов в доменных зонах, на которые не распространяются полномочия ФинЦЕРТ как организации, компетентной в определении нарушений, осложняет возможность приостановки деятельности таких ресурсов, связанной с распространением ВПО. В настоящий момент прорабатывается законопроект, наделяющий Банк России правом досудебной блокировки таких сайтов на территории Российской Федерации вне зависимости от географической привязки доменного имени.

ТРЕНДЫ ГОДА

- К концу 2018 г. основной вектор наиболее опасных атак на организации кредитно-финансовой сферы сместился в сторону кредитных организаций ряда стран СНГ. Основной атакуемой системой, как и в предыдущем году, оставался процессинг банковских карт. Атакующие пытаются добраться до интерфейса системы управления процессинга независимо от ее типа либо до сервера баз данных, чтобы скрытно увеличить балансы и лимиты заранее подготовленных и находящихся в распоряжении их сообщников карт. Затем по этим картам снимаются все доступные денежные средства через банкоматы не только различных банков, но и иногда в разных странах.
- По-прежнему распространены атаки на устройства самообслуживания, осуществляемые, как правило, неустойчивыми малыми группами либо одиночками. При этом скимминг и шимминг идут на убыль, среди традиционных атак позиции сохраняют только blackbox-атаки с использованием специализированных устройств.

- В атаках не на непосредственно кредитно-финансовые организации, а на их клиентов (юридических лиц) злоумышленники, как правило, уделяют меньше внимания подготовке сложного инструментария, чем подготовке атаки с точки зрения социальной инженерии.
- В случаях, когда злоумышленники, проведя предварительную разведку в сети атакованной организации, осознавали, что потенциальная выгода достаточно объемна, они переходили к использованию более сложных инструментов – возможно, обращаясь к опыту «старших братьев», атакующих сложные системы защиты организаций кредитно-финансовой сферы.
- Среднее зафиксированное время от момента первичной компрометации инфраструктуры кредитной организации до момента хищения – 20–30 календарных дней. Однако в 2018 г. было зафиксировано и несколько случаев хищения, когда от момента заражения до момента хищения проходило более полугода. Это связано с тем, что атакованная организация либо изначально была не слишком интересна злоумышленникам и присутствие вредоносных программ в ее информационной системе сохранялось в качестве резерва, либо атакующие не могли подобрать работающий способ вывода денежных средств, что особенно характерно для кредитных организаций, не имеющих собственного процессинга платежных карт.
- Крайне высокую интенсивность сохраняют кампании по распространению вредоносного программного обеспечения класса ransomware. В дальнейшем стоит опасаться использования авторами данного класса ВПО уязвимостей, подобных выявленной в текущем году CVE-2019-0708 в службах удаленного рабочего стола Windows. Подобные уязвимости исключают участие пользователя атакуемого компьютера в процессе заражения и могут стать причиной масштабных эпидемий, приводящих к внушительным затратам на ликвидацию последствий.

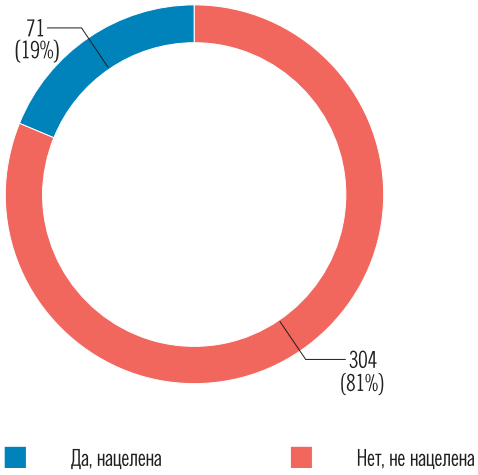
АТАКИ НА ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ ОРГАНИЗАЦИЙ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Прямые атаки непосредственно на организации кредитно-финансовой сферы являются современным аналогом ограблений казначейств и банков, хорошо известных человечеству хотя бы по художественным фильмам жанра вестерн. Традиционно кредитно-финансовые организации представляют собой объекты, обладающие одной из наиболее высоких степеней защищенности. В случае с компьютерными атаками речь идет о защищенности информационной инфраструктуры. Сегодня мировое сообщество прикладывает значительные усилия к обеспечению экономической безопасности, в том числе в информационной ее части, но тем не менее прямые проникновения в информационно-телекоммуникационные сети кредитно-финансовых организаций с последующим выводом денежных средств остаются достаточно частым и опасным явлением.

По перечисленным выше причинам злоумышленники, проводящие атаки на такие организации, как правило, действуют хорошо организо-

ванными группами, по крайней мере в части ядра данных групп. Такие группы, по версиям правоохранительных органов и экспертов в области компьютерной безопасности, как правило, включают нескольких организаторов на стратегическом уровне принятия решений, нескольких инсайдеров кредитно-финансовой сферы (из числа действующих либо бывших сотрудников), а также нескольких достаточно квалифицированных технических специалистов. При этом перечисленные подгруппы могут пересекаться и входить одна в другую. Черновую работу, такую как снятие наличных денежных средств, в основном поручают каждый раз разным людям – так называемым «дропам» («мулам»), не связанным с ядром группы напрямую и найденным на соответствующих ресурсах в сети Интернет либо в ее теневом сегменте, известном как Darknet. При этом целями атак, как правило, являются информационные системы, позволяющие осуществлять хищения в крупных объемах: автоматизированное рабочее место клиента Банка России (АРМ КБР), системы процессинга платежных карт, шлюзы платежных систем. Только в отдельных случаях (вероятно, когда злоумышленникам не удается проникнуть в критические узлы информационной системы) итоговой целью становится подсеть устройств самообслуживания с последующей установкой на устройства специализированного ВПО для выдачи наличных «дропам» по переданному организаторами атаки ключу.

Нацеленность зафиксированных атак на организации КФС и их клиентов



Из 375 кампаний по распространению ВПО, зафиксированных ФинЦЕРТ, 71 была нацелена конкретно на организации кредитно-финансовой сферы и их клиентов (см. раздел «Атаки на информационную инфраструктуру юридических лиц – клиентов организаций кредитно-финансовой сферы»).

На протяжении 2018 г. ФинЦЕРТ Банка России многократно фиксировал целевые атаки на организации кредитно-финансовой сферы, приписываемые двум основным преступным группам – Cobalt (также известна

как Carbanak и FIN7) и Silence. Первая группа получила свое название по имени программного обеспечения для тестирования информационных систем на проникновение Cobalt Strike, производимого американской компанией Strategic Cyber, LLC. Вторая группа использует вредоносное программное обеспечение собственной разработки, получившее название Silence от одного из производителей антивирусного программного обеспечения, впервые его выявившего.

Несмотря на арест в марте 2018 г. в Испании одного из лидеров Cobalt и задержание в Европе еще нескольких ее членов, группа свою деятельность не прекратила, а лишь снизила активность на некоторое время.

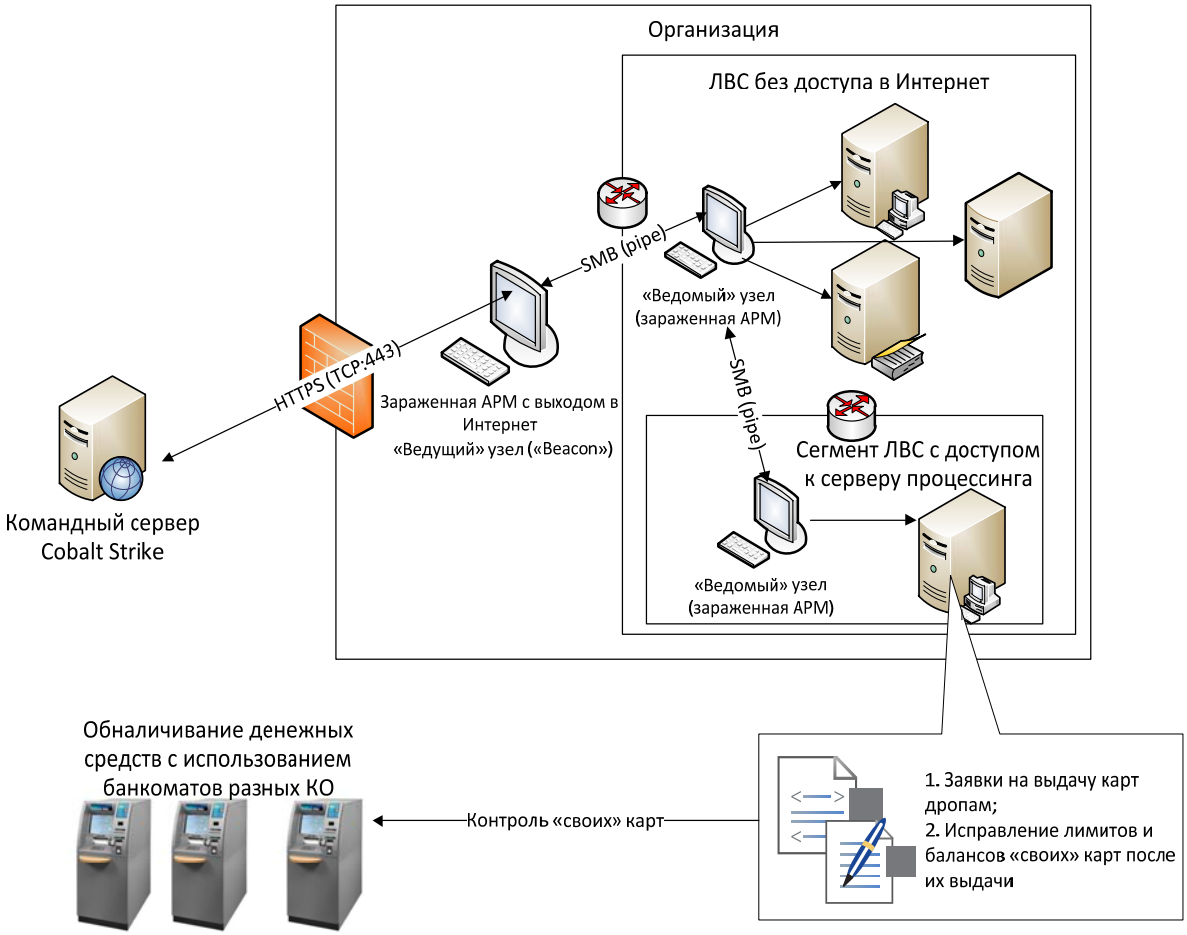
Необходимо отметить, что у специалистов ФинЦЕРТ есть основания полагать, что после громких арестов от группы могла отделиться часть, на данный момент сформировавшаяся в самостоятельное, аналогичное по степени квалифицированности и опасности сообщество, не привязанное к каким-то определенным инструментам атак либо меняющее их в целях затруднения классификации своих атак специалистами по безопасности. На текущий момент активность этой новой группы не так широка, но теоретически будет нарастать.

В последующем интенсивность атак «основной» части группы Cobalt восстановилась. В середине года поступали сообщения о многочисленных атаках группы на банки дальнего зарубежья.

Тактика работы групп Silence, Cobalt и им подобных весьма схожа: первоначальное проникновение идет через spear-phishing письма, рассылаемые по списку электронных адресов сотрудников организаций. Часто письма направляются якобы от имени каких-либо других финансовых организаций или от имени органов государственной власти. ВПО обычно содержится во вложениях таких писем. Чуть реже используется вариант, когда файл предлагается загрузить с какого-либо внешнего ресурса по ссылке из тела письма, например с облачных сервисов поисковых систем. После открытия вложения или загруженного файла (чаще всего документа формата программного пакета Microsoft Office) скрытно происходят загрузка и запуск программного обеспечения, предоставляющего атакующим удаленный доступ к компьютеру. В абсолютном большинстве известных случаев для внедрения кода использовались уязвимости указанного программного пакета, такие как CVE-2017-11882, CVE-2018-0802 и иные, ранее уже устраненные в выпущенных Microsoft обновлениях. Иными словами, успех атакующих в том числе обусловлен использованием несвоевременно обновляемого и сохраняющего широко известные уязвимости программного обеспечения, установленного на АРМ сотрудников организаций.

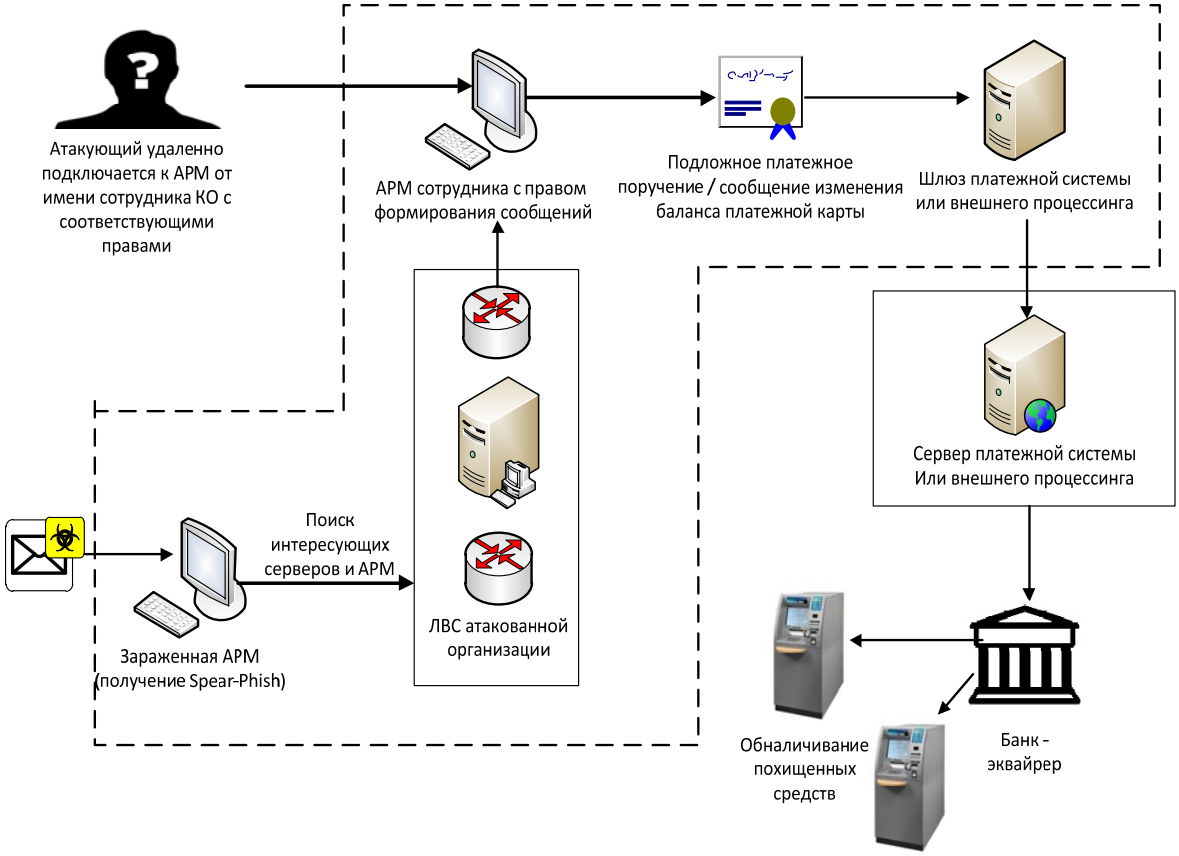
После проникновения на первый компьютер атакующие проводят изучение доступного сегмента локальной сети, выявляют другие представляющие интерес АРМ и серверы, проникают и закрепляются на них, а затем приступают к подготовке хищения.

Принципиальная схема атаки значимых изменений с 2017 г. не претерпела.



В случае если у атакованной организации нет своего процессинга, но есть платежный шлюз, атакующие используют его для передачи подложных платежных поручений либо поручений для изменения баланса платежных карт (при использовании процессинговых центров).

Вариант принципиальной схемы атаки на инфраструктуру КФО при отсутствии собственного процессинга



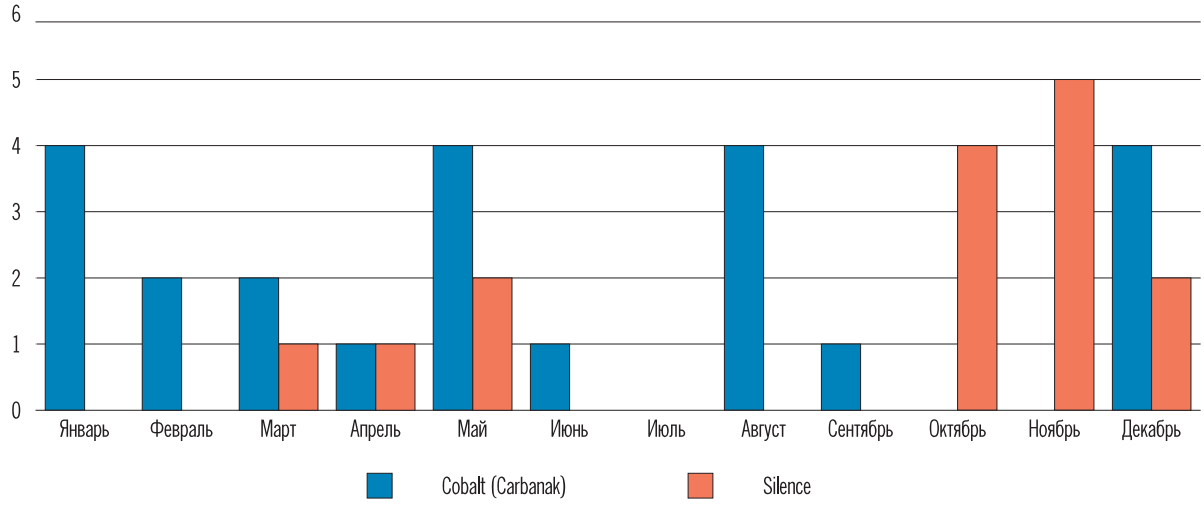
Здесь стоит упомянуть, что одним из возможных и, пожалуй, самым простым вариантом достижения итоговых целей атак является компрометация подсети устройств самообслуживания (банкоматов) с загрузкой на такие устройства специализированного ВПО. Данный вариант, как правило, использовался атакующими в случаях исчерпания иных возможностей вывода денежных средств. Одним из наиболее распространенных видов этого ВПО в конце 2017 – начале 2018 г. стала программа Cutlet Maker, подробно описанная в ежегодном отчете ФинЦЕРТ[2]. Отдельные преступные группы могут использовать ВПО собственной разработки, такое как ATMitch, для отдачи команд диспенсерам банкоматов на выдачу наличных денежных средств.

Специалистами ФинЦЕРТ также отмечен возросший профессионализм организаторов вредоносных рассылок: они стали более убедительными как с точки зрения соблюдения деловой стилистики, так и с точки зрения грамматики. Практически все рассылки выполняются с использованием либо спуфинга (подмены) адреса отправителя, либо специально созданного ресурса, либо ранее скомпрометированного почтового сервера или почтового ящика какой-либо известной организации. Отмечены также

[2] *Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России 1.09.2017 – 31.08.2018, раздел «Атаки на устройства самообслуживания», http://www.cbr.ru/fincert/.*

случаи использования почтовых сервисов организации, в которой ранее было успешно совершено хищение денежных средств.

Количество атак групп Cobalt и Silence в 2018 году



Любопытно, что по статистике 2017–2018 гг. наибольшее число успешных хищений происходило после атак, проведенных в «отпускные» месяцы – с мая по август. Это может быть связано со снижением бдительности сотрудников организаций. Вероятно, находясь в ожидании отпуска или в расслабленном состоянии после него, сотрудники чаще открывают файлы из писем, пришедших из неизвестных источников.

К концу 2018 г. возросла активность группы Silence, которая постепенно наращивала интенсивность атак на российские кредитно-финансовые организации, имела ряд значимых успехов и, вероятно, в будущем также будет представлять значительную опасность.

Возможно, во многом благодаря успешным хищениям наблюдалось увеличение числа атак в октябре-ноябре. После совершения хищений из российской кредитной организации с использованием ее сервера электронной почты были несколько раз осуществлены вредоносные рассылки по адресам кредитных организаций России и стран СНГ.

Согласно данным ФинЦЕРТ, ущерб российских организаций кредитно-финансовой сферы в 2018 г. от атак группы Cobalt составил не менее **44 млн руб.**, а от атак, которые, как предполагается, были осуществлены группой Silence, – не менее **14 млн 403 тыс. рублей**. Однако даже в сумме это во много раз меньше, чем ущерб от таких же целевых атак в 2017 г., что, к сожалению, не означает такого же снижения самой опасности целевых атак. Основными факторами, способствовавшими их успешности, являются:

– отсутствие своевременного обновления антивирусного программного обеспечения на АРМ пользователей;
– отсутствие актуальных патчей безопасности распространенного офисного программного обеспечения, в частности пакета Microsoft Office;

– отсутствие актуальных патчей безопасности операционных систем, эксплуатация не поддерживаемого производителем программного обеспечения (end-of-life);
– массовое использование учетных записей с привилегиями локальных администраторов, необоснованное назначение повышенных привилегий пользователям в различных информационных системах;
– отсутствие контроля доступа либо логирования доступа пользователей к критичным для организации информационным системам (процессинг карт, любые системы переводов денежных средств);
– нарушение пользователями правил информационной безопасности, например постоянное подключение второго фактора (токена) к АРМ, с которого возможно формирование платежных поручений, либо доступ с повышенными привилегиями к критичным информационным системам;
– использование простых паролей;
– использование уязвимых конфигураций домена Active Directory, например назначение локальных администраторов политиками домена;
– наличие доступа в сеть Интернет в обход межсетевых экранов или вообще неконтролируемого доступа в сеть Интернет.

К факторам, затрудняющим обнаружение и реагирование на атаку, относятся:

– отсутствие протоколирования либо недостаточная длительность хранения логов сетевых соединений пограничного устройства;
– отсутствие периодических проверок на известные индикаторы компрометации систем и сетей (IOC). В некоторых случаях – отсутствие заранее определенных мер реагирования на инциденты при обнаружении реагирования на индикаторы компрометации;
– отсутствие средств обнаружения вторжений (IDS), деактивированные сигнатуры обнаружений следов работы программ типа Mimikatz, Meterpreter;
– наличие большого числа установленных средств удаленного администрирования наподобие TeamViewer, RAdmin;
– отсутствие единого списка разрешенного к использованию программного обеспечения, несвоевременная актуализация подобного списка, что сильно затрудняет обнаружение и удаление программ, установленных атакующими;
– сохраненные без шифрования пароли доступа к критичным информационным системам (например, в ряде случаев пароли хранились в текстовых файлах на рабочих столах администраторов и руководителей);
– нежелание привлекать специализированные экспертные организации, в том числе ФинЦЕРТ, для оказания помощи в случаях выявления заражений и неспособности справиться с ним самостоятельно;

– сокрытие от ФинЦЕРТ факта компрометации (в этом случае увеличивается вероятность потери денежных средств, поскольку ФинЦЕРТ не может заблаговременно принять меры по задержанию переводов денежных средств).

Подытоживая информационный блок ФинЦЕРТ о целевых атаках на организации кредитно-финансовой сферы, необходимо отметить также не менее двух фактов успешного снятия в банкоматах российских кредитных организаций крупных сумм денежных средств, похищенных у иностранных банков группой Lazarus (Hidden Cobra, APT 38). Средства и методы, использованные преступниками, могут быть применены и против российских организаций, в связи с чем ФинЦЕРТ внимательно отслеживает результаты ведущихся расследований.

АТАКИ НА ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ ЮРИДИЧЕСКИХ ЛИЦ – КЛИЕНТОВ ОРГАНИЗАЦИЙ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ

С технической точки зрения атаки на клиентов финансовых организаций в основном отличаются меньшей сложностью используемого инструментария – соответственно, для их осуществления требуется более низкая квалификация самих атакующих, меньший организационный ресурс. По версии специалистов ФинЦЕРТ, подобные атаки проводятся чаще всего организованными группами, но такие группы обладают меньшей стабильностью и устойчивостью состава в отличие от атакующих непосредственно организации кредитно-финансовой сферы. Также наблюдается склонность атакующих к более частой смене инструментов достижения целей, которыми в свою очередь являются выходные точки из организации на обслуживающую ее организацию кредитно-финансовой сферы, то есть бухгалтерские и иные финансовые подразделения юридических лиц. Целью может стать соответствующее программное обеспечение для проведения платежей либо сервисы электронной почты, если после изучения инфраструктуры злоумышленники выясняют, что осуществить перечисление денежных средств возможно, подделав соответствующие письма внутри или вовне организации. При этом общая схема атаки зачастую совпадает с аналогичной для компрометации ресурсов и сетей организаций кредитно-финансовой сферы, отличается лишь конечная цель. По некоторым данным, возможно также сделать предположение о том, что подобные атаки могут организовываться отдельными членами известных групп злоумышленников, атакующих банки, в периоды, свободные от занятости по основному направлению.

Единственный способ компрометации систем организаций – клиентов банков, отмеченный ФинЦЕРТ в 2018 г. как разительно отличающийся от классических атак на организации кредитно-финансовой сферы, – тех-

ника watering hole[3]. К примеру, было зафиксировано несколько кампаний по распространению ВПО семейства Buhtrap посредством атак watering hole. Указанная схема заражения также неоднократно выявлялась специалистами ФинЦЕРТ при проведении исследований носителей информации, подвергшихся воздействию ВПО для совершения хищений денежных средств.

PowerShell-загрузчик Buhtrap и содержимое cookie-файла, связанного с его появлением в атакованной системе

```
$global:Url    = "https://[redacted]/blog/attachment.php?attachmentid=38606"
$global:Hash   = "d41d8c"
$global:Temp   = $env:TEMP
$global:Cache  = $FALSE
$global:Binary = $TRUE

function Create-Temp-Folder
{
    $IO   = [System.IO.Directory]
    $Name = ("scp" + (Get-Random -Minimum 9999 -Maximum 99999))

    if ($IO::CreateDirectory("$global:Temp\$Name"))
    {
        (Se
    }
}

function Cr
{
    if ($gl
    {
        $Na

        if (($Name.length) -eq 6)
        {
            $Path = "$global:Temp\$Name.tmp"
```

```
1
[redacted]/buh/articles/42369/
9216
1545622016
30654679
3160206315
30653270
*
```

Также в атаках на юридические лица использовалось ВПО семейства TeamBot, основанное на легальном ПО для удаленного администрирования компьютера TeamViewer. В таких атаках ПО TeamViewer, как правило, дополнительно модифицировалось для скрытой работы с целью минимизации вероятности визуального обнаружения легитимными пользователями. Векторы проникновения в таких случаях были различными – от схем, аналогичных кампаниям по распространению Buhtrap через популярные порталы, до атак spear-phishing посредством электронной почты. В последних использовалось направление на адреса электронной почты, предположительно принадлежавшие, по мнению атакующих, финансовым подразделениям юридических лиц, сообщений, текст которых подготовлен с использованием приемов социальной инженерии. Приложение к электронному письму содержит загрузчик программного модуля ВПО либо программу-контейнер, непосредственно устанавливающую модуль ВПО в систему, извлекая его из собственного тела.

При этом атакующими для сокрытия факта загрузки из сети Интернет на атакованный компьютер программных модулей ВПО используются раз-

[3] *Взлом популярных сайтов заданной направленности (в случае с сотрудниками финансовых подразделений – СМИ и порталов бухгалтерской/экономической направленности) с последующим размещением на них вредоносного программного кода, предназначенного для загрузки на средства вычислительной техники при заходе на взломанный ресурс пользователей – целей атаки.*

личные техники, такие как помещение модулей в архивный файл, который маскируется под файл изображения формата JPEG, загружается в таком виде на атакуемый компьютер – и там уже распаковывается как обычный архив.

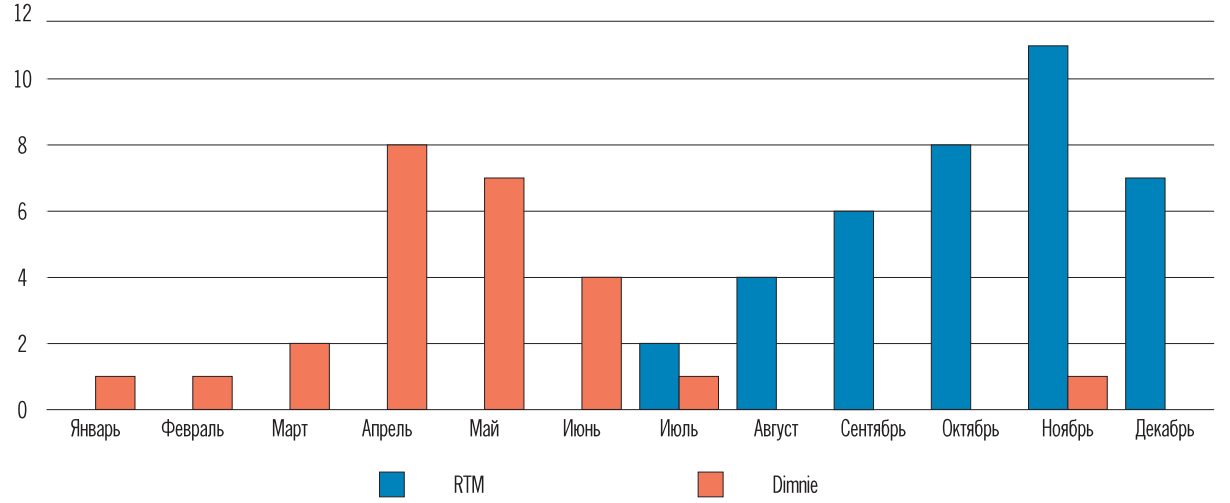
Файлы ВПО TeamBot, извлеченные из псевдо-JPEG-файла

Имя	Размер	Сжатый	Изменен
x64	132 044	0	2016-10-19 15:31:10
x86	96 990	0	2016-10-19 15:31:09
fkoiei8lfuc	44 544	488 096	2017-04-20 17:19:00
installvpn.pg	3 585		2016-10-03 19:31:32
lsz2unuxsh7moh.jpg	7 838		2017-04-20 17:51:06
msoobe.exe	7 293 280	2 315 856	2013-02-19 14:02:00
rdw.pg	415 745		2016-06-08 12:06:31
scankey.pg	2 049		2016-10-03 19:31:32
TeamViewer_Desktop.exe	2 163 040		2013-02-19 14:02:01
TeamViewer_Resource_en.dll	1 276 256		2013-02-19 14:02:08
tv.cfg	1 346		2017-04-20 17:55:07
tv_w32.dll	50 528		2013-02-19 11:59:12
tv_w32.exe	108 896		2013-02-19 11:59:12
tv_x64.dll	53 600		2013-02-19 11:59:13
tv_x64.exe	144 736		2013-02-19 11:59:13
update.pg	19 969		2016-12-31 01:57:30

Стоит еще раз подчеркнуть, что группы атакующих не зациклены на использовании одних и тех же инструментов. Наряду с ВПО TeamBot, активно использовалось также соответствующим образом модифицированное ПО для удаленного администрирования LiteManager и иные подобные программные продукты.

Однако наиболее активно в 2018 г. для первичной компрометации отдельных компьютеров и информационных сетей юридических лиц, а в отдельных случаях и непосредственно для осуществления хищений использовалось ВПО семейств RTM и Dimnie.

Выпуск бюллетеней ФинЦЕРТ по фактам распространения ВПО семейств RTM и Dimnie в 2018 году



При этом, как видно из приведенной статистики, кампании по распространению ВПО указанных семейств перетекают одна в другую, практически не пересекаясь. Это обстоятельство, а также различные совпадения в действиях атакующих позволяют сделать обоснованное предположение о том, что оба вида ВПО используются одной и той же группой.

Злоумышленники периодически уделяли большое внимание предварительной подготовке и применению методов социальной инженерии. Так, в одном из известных ФинЦЕРТ случаев атакующими был произведен взлом почтового сервера организации, имеющей множество различных корреспондентов среди иных юридических лиц, а затем – рассылка программы-контейнера («дроппера») RTM по списку корреспондентов организации от имени ее сотрудников. Таким образом, атакующими был достигнут повышенный уровень доверия среди получателей вредоносных писем и высокий процент запуска получателями программ – контейнеров ВПО.

Несмотря на направленность атак с использованием ВПО данных семейств не на сами кредитно-финансовые организации, а на их клиентов, предположительная небрежность составления списков рассылки из расчета на случайный успех атаки приводила к попаданию писем на почтовые адреса банков и последующей пересылке профильными специалистами на анализ в ФинЦЕРТ.

Объединяющим эти два семейства техническим признаком является периодическое использование с целью взаимодействия экземпляров ВПО с командными серверами системы доменных имен NameCoin. NameCoin представляет собой альтернативную анонимную децентрализованную систему DNS-серверов, построенную на основе технологии блокчейн, и позволяет скрывать данные о разрешенных доменом IP-адресах. Подробную информацию о системе NameCoin в связи с участившимися рассылками ВПО семейства RTM ФинЦЕРТ публиковал в информационном бюллетене в октябре 2018 года. Также отмечен период использования

авторами и операторами ВПО семейства RTM управляющих центров, расположенных в сети TOR.

Стоит отметить, что даже новые экземпляры ВПО указанных семейств обычно имеют высокий уровень детектируемости популярным антивирусным программным обеспечением. При этом первичное проникновение часто осуществляется за счет эксплуатации уязвимостей, информация о которых давно опубликована (как и в случае с атаками непосредственно на кредитно-финансовые организации), либо с использованием программ-контейнеров, детектирующихся эвристически почти всеми популярными антивирусными программами. Таким образом, наиболее эффективный метод противодействия подобным атакам зачастую заключается в поддержании антивирусных баз в актуальном состоянии и своевременном обновлении используемого программного обеспечения – как системного, так и прикладного.

Интересным фактом является то, что модули ВПО указанных семейств регулярно встречались специалистам ФинЦЕРТ в ходе исследования подвергшихся воздействию ВПО носителей информации, проводившегося в интересах правоохранительных органов, по следам реально произошедших хищений денежных средств. Причем встречались они в сочетании с иными инструментами.

Так, в одном из проведенных специалистами ФинЦЕРТ исследований на компьютере пострадавшей организации, в том числе в карантине антивирусного ПО, были одновременно обнаружены программные модули ВПО семейств Dimnie, Buhtrap и CobInt[4]. Возможно, что ВПО Dimnie использовалось с целью предварительной разведки степени защищенности организации. После осознания того факта, что в организации все же присутствует установленное антивирусное программное обеспечение, атакующие переключились на использование более сложных инструментов, таких как Buhtrap.

В другом случае в системе был выявлен установленный и не удаленный антивирусом основной модуль Dimnie, отвечающий за загрузку на компьютер иных модулей ВПО. А вскоре после доставки программы-контейнера, устанавливающей в систему основной модуль Dimnie, в файловой системе были выявлены первые следы ВПО семейства Buhtrap. Таким образом, в данном случае атакующими, вероятно, изначально предполагалось использование ВПО Dimnie для первичной компрометации и доставки ВПО иных семейств.

После установки в систему средств удаленного администрирования либо основанных на ВПО (например, Buhtrap), отдельные модули которого предоставляют удаленное управление компьютером, либо иных программных продуктов (таких как LiteManager) начиналось взаимодействие с инфраструктурой – управляющими серверами – атакующих. В его ходе атакующие исследовали зараженный компьютер, определяли, имеет ли отношение деятельность его пользователя к финансам, и при положительном результате осуществляли хищение, либо в ручном режиме рабо-

[4] *CobInt – семейство ВПО, построенного на основе программного обеспечения Cobalt Strike.*

тая с соответствующим финансовым ПО, либо подгружая на захваченный компьютер модуль ВПО, который осуществлял подмену бухгалтерских реквизитов в (полу)автоматическом режиме.

Руководству организаций – клиентов учреждений кредитно-финансовой сферы на данный момент необходимо уделять внимание вопросу повышения грамотности персонала в области информационной безопасности. Большинство атак на юридические лица рассчитаны на низкий уровень компьютерной грамотности либо на невнимательность атакуемых сотрудников. Таким образом, привитая персоналу осторожность и осмотрительность в вопросах использования электронной почты и иных ресурсов в сети Интернет часто играет решающую роль в предотвращении реализации угроз безопасности. При этом, разумеется, не следует забывать и про современную и достаточно надежную систему антивирусной защиты, как и про средства защиты от сетевых атак, устанавливаемые непосредственно на каналах доступа в сеть организации извне.

Самим организациям кредитно-финансовой сферы также стоит уделить внимание совместной работе со своими клиентами по линии повышения их осведомленности в области безопасности (security awareness). Это может достигаться различными путями, в том числе посредством проведения соответствующих тренингов по тематике информационной безопасности систем онлайн-банкинга на базе организации кредитно-финансовой сферы.

АТАКИ НА УСТРОЙСТВА САМООБСЛУЖИВАНИЯ

Под атаками, целями которых являются конкретно устройства банковского самообслуживания (АТМ), специалистами ФинЦЕРТ в данном разделе обзора подразумеваются не атаки, где АТМ становятся лишь точкой вывода средств в общей схеме более масштабной атаки, а атаки, где АТМ являют собой зачастую и точку входа для злоумышленников, и конечную цель. Подобные атаки осуществляются, как правило, не в рамках сложно организованных и/или массовых вредоносных кампаний, а эпизодически. Злоумышленниками в таких случаях часто становятся одиночки или неустойчивые, хаотически собранные небольшие группы, осуществляющие несколько подобных атак и потом «залегающие на дно» либо расформировывающиеся.

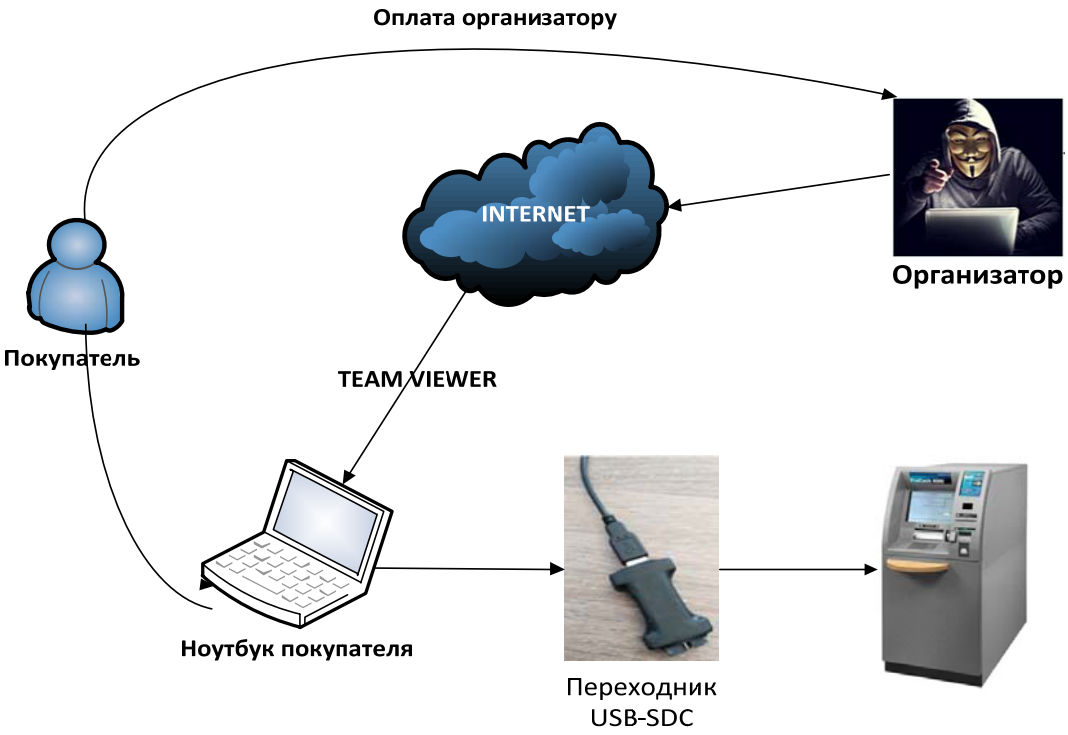
Основные виды атак на устройства самообслуживания каких-либо значительных изменений в 2018 г. не претерпели. В России по-прежнему фиксируются атаки типа blackbox, а также попытки атак типа «прямой диспенс».

Атака blackbox обычно начинается со вскрытия передней панели банкомата и подсоединения некоего стороннего устройства. Чаще всего такое устройство представляет собой переходник – конвертер интерфейсов, например USB-RS485[5]. Переходник через USB-кабель подключается к портативному компьютеру. Как правило, это недорогие, бывшие в употреблении нетбуки, которые злоумышленникам не жалко бросить

[5] *Сервисный интерфейс, который часто используется в старых банкоматах.*

на месте проведения атаки. На компьютере установлена программа удаленного администрирования, например TeamViewer, с помощью которой подключается находящийся на удалении сообщник (либо организатор), запускающий программу, которая взаимодействует с диспенсером банкомата. От подобного рода воздействий может дополнительно защитить включение шифрования данных, передаваемых между диспенсером и системным блоком банкомата, однако на старых банкоматах или расположенных в удаленных от федерального центра регионах оно применяется не всегда.

Схема реализации атаки с использованием blackbox



Ожидавшийся ранее всплеск TRF-атак (transaction reversal fraud – мошенничество с отменой транзакций) не произошел, однако был зафиксирован новый способ такой атаки, основанный на несовершенстве сценариев обработки переводов с карты на карту с использованием банкоматов.

Упрощенно данный вид TRF-атаки выглядит следующим образом:

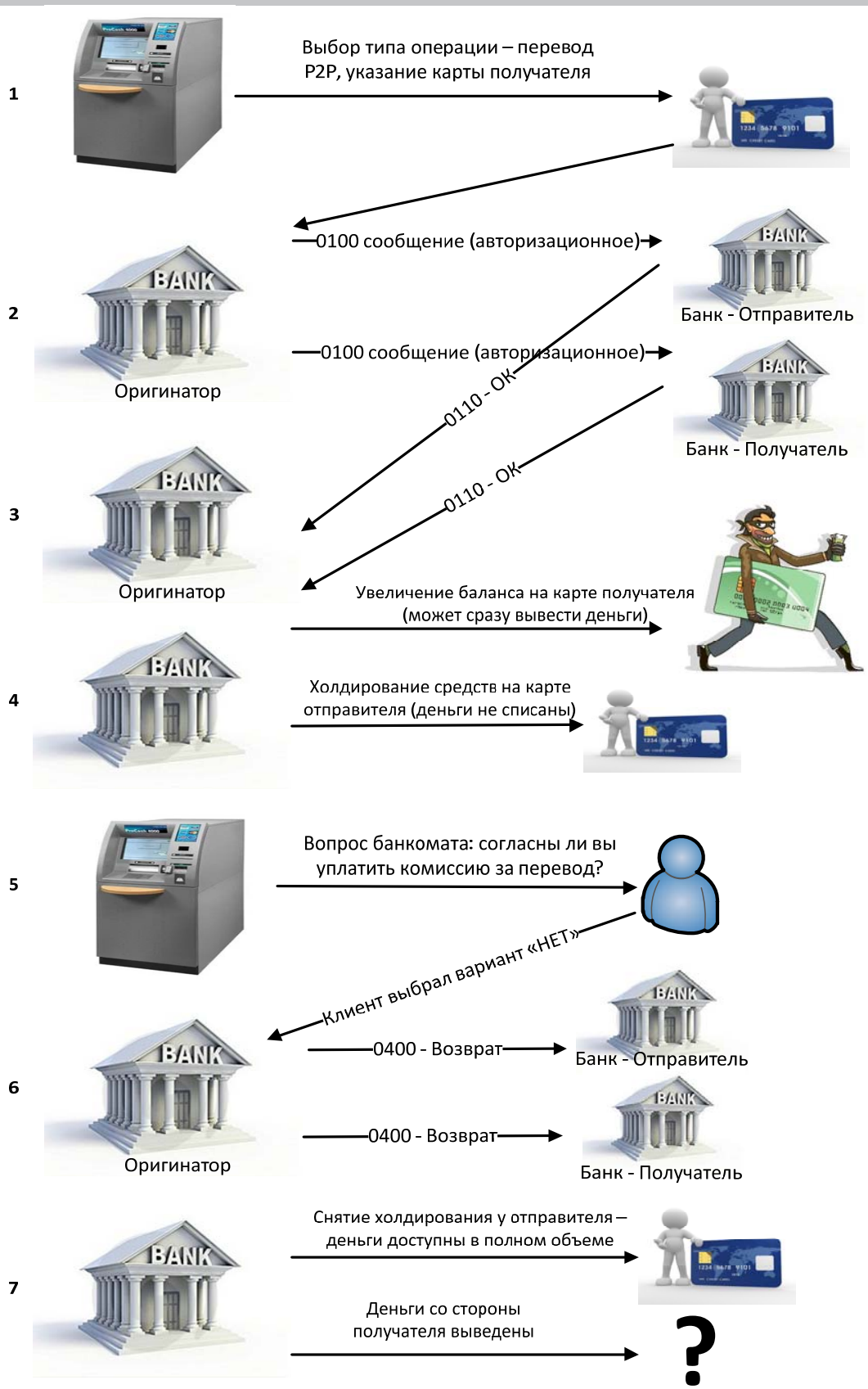
– в банкомате выбирается тип операции – перевод P2P (от клиента к клиенту), указывается номер карты получателя;
– банк-инициатор[6] **одновременно** направляет два авторизационных сообщения: банку-получателю и банку-отправителю;
– инициатору **практически одновременно** приходит одобрение от обоих банков (в случае, если операция возможна – имеется не-

[6] *Банк, инициировавший операцию. В контексте: банк – владелец устройства самообслуживания.*

обходимое количество денежных средств на балансе карты отправителя и так далее);

– выполняется фактический перевод: увеличивается сумма на карте получателя, одновременно с этим холдируется такая же сумма у отправителя. Сценарий P2P-перевода в банкомате при этом **еще не закончен**!
– банкомат «спрашивает» у отправителя о согласии на списание комиссионных за операцию;
– отправитель **не соглашается**, поэтому банк-инициатор отправляет сообщение о возврате в банк-отправитель и банк-получатель;
– холд со счета отправителя **снимается**, вместе с тем средства уже **выведены** получателем.

Схема атаки


1
Выбор типа операции – перевод P2P, указание карты получателя
2
0100 сообщение (авторизационное)
Банк - Отправитель
Оригинатор
0100 сообщение (авторизационное)
0110 - ОК
Банк - Получатель
3
0110 - ОК
Оригинатор
Увеличение баланса на карте получателя (может сразу вывести деньги)
4
Холдирование средств на карте отправителя (деньги не списаны)
5
Вопрос банкомата: согласны ли вы уплатить комиссию за перевод?
Клиент выбрал вариант «НЕТ»
6
0400 - Возврат
Банк - Отправитель
Оригинатор
0400 - Возврат
Банк - Получатель
7
Снятие холдирования у отправителя – деньги доступны в полном объеме
Деньги со стороны получателя выведены
?

Основным способом минимизации рисков такой атаки является проверка корректности сценария работы банкомата. Для банка – владельца АТМ – мониторинг операций типа Reversal, а также следующие изменения в сценарии: отправка сообщения 0400 «Возврат» в банк отправителя должна происходить **строго после** успешного завершения операции 0400 «Возврат» в сторону банка получателя.

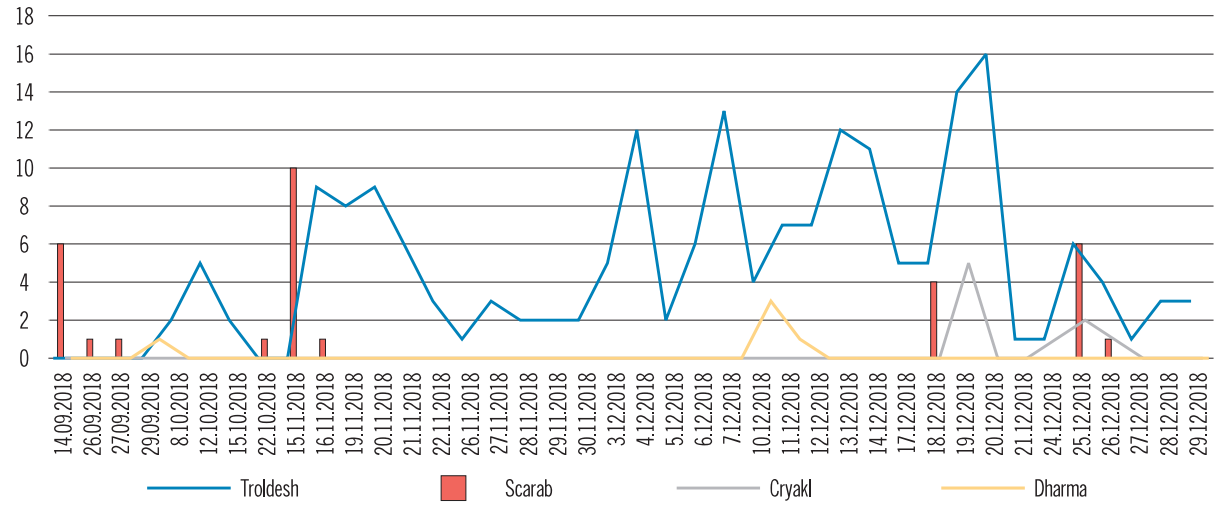
Также довольно эффективной мерой является получение согласия клиента с условиями обслуживания до отправки авторизационных сообщений.

АТАКИ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Программы-вымогатели (ransomware, далее по тексту – шифровальщики в связи с наиболее часто используемой схемой вымогательства) заслужили отдельного упоминания из-за частоты и массовости кампаний по их распространению. Несмотря на то, что в 2018 г. не зафиксировано резонансных и успешных для злоумышленников кампаний по распространению шифровальщиков, как это было годом ранее, число атак на организации кредитно-финансовой сферы России с использованием различных шифровальщиков существенно возросло.

До запуска в сентябре 2018 г. АСОИ ФинЦЕРТ от участников информационного обмена по электронной почте поступило свыше 100 сообщений о зафиксированных случаях рассылки программ-шифровальщиков. Оперативные бюллетени подготавливались и направлялись 17 раз по наиболее опасным из этих атак. С сентября по декабрь 2018 г. через АСОИ ФинЦЕРТ было получено 274 запроса, содержащих информацию о 195 зафиксированных случаях рассылки программ-шифровальщиков.

Количество обработанных запросов в отношении различных семейств программ-шифровальщиков за сентябрь-декабрь 2018 года



Большая часть запросов участников информационного обмена была связана с распространением шифровальщиков семейств Troldesh (также известен как Shade/Purga), Scarab, Cryakl и Dharma.

Основным способом распространения шифровальщиков является рассылка по электронной почте сообщений, содержащих во вложении либо программу-загрузчик, осуществляющую скачивание и установку в операционную систему основного программного модуля, либо непосредственно основной модуль ВПО. В сообщениях, направляемых в адрес организаций кредитно-финансовой сферы, используется схожий стиль оформления: сообщения поступают якобы от имени организаций кредитно-финансового сектора, авиакомпаний и крупных компаний иных отраслей. Для рассылки писем используются скупаемые мелким оптом на черном рынке аккаунты электронной почты самых различных по расположению и личной или корпоративной принадлежности пользователей, в связи с чем адреса отправителей часто удивляют получателей. Также используется спуфинг адресов. Тематика сообщений – документы, чаще всего некие заказы. Пояснительный текст очень короток, и, как правило, он содержит явные орфографические ошибки и пытается прямо побудить пользователя открыть файл в приложении.

Специалистами ФинЦЕРТ ранее были выпущены и распространены посредством АСОИ подробные бюллетени с рекомендациями по противодействию и восстановлению данных, посвященные двум наиболее часто встречающимся семействам ВПО данного класса – Scarab и Troldesh.

РЕКОМЕНДАЦИИ ФИНЦЕРТ

Для снижения риска успешной реализации атак необходимо:

– использование и своевременное обновление современного антивирусного программного обеспечения на АРМ пользователей и серверах;
– своевременная установка исправлений (patch-management) безопасности распространенного офисного программного обеспечения, в частности пакета Microsoft Office;
– своевременная установка исправлений (patch-management) безопасности операционных систем, своевременный вывод из эксплуатации неподдерживаемого производителем программного обеспечения (end-of-life) в случае наличия такой возможности;
– использование учетных записей с минимально необходимыми для работы пользователя привилегиями, ограничение количества учетных записей локальных администраторов, исключение необоснованного назначения повышенных привилегий пользователям в различных информационных системах;
– контроль/логирование доступа пользователей к критичным для организации информационным системам (процессинг карт, любые системы переводов денежных средств);
– проведение регулярных тренингов с пользователями внутри организации и с представителями организаций-клиентов по линии ос-

ведомленности в области информационной безопасности (security awareness);
– при наличии возможности проведение полноценных «киберучений», проверяющих готовность персонала противостоять атакам на информационную инфраструктуру организации, а также устойчивость к атакам с использованием социальной инженерии;
– качественные парольные политики (необходимо исключить использование сотрудниками паролей, не соответствующих требованиям безопасности);
– необходимо исключить применение уязвимых конфигураций домена Active Directory, например назначение локальных администраторов политиками домена; целесообразно использовать «лучшие практики» (Best Practices) от производителя при конфигурировании домена. Также по возможности целесообразно отказываться от применения старых (2003–2008 гг.) схем Active Directory и использовать контроль учетных записей пользователей, предлагаемый новыми схемами;
– необходимо исключить наличие в организации неконтролируемых каналов доступа в сеть Интернет (в обход межсетевых экранов и иных программно-аппаратных средств контроля и ограничения).

Для улучшения процессов обнаружения и реагирования на атаки необходимо:
– вести протоколы (журналы, логи) сетевых соединений пограничного с сетью Интернет устройства, установить разумный и достаточный период их хранения, но не менее 3 месяцев (90 дней);
– проводить периодические проверки инфраструктуры по известным индикаторам компрометации систем и сетей (IOC). Разработать и применять соответствующие процедуры реагирования в случаях выявления срабатываний по индикаторам;
– ввести в эксплуатацию средства обнаружения вторжений (IDS), содержащие сигнатуры обнаружения следов работы часто использующегося атакующими программного обеспечения, такого как Mimikatz, Meterpreter и так далее; убедиться, что данные сигнатуры активны и что возможно постоянное обновление сигнатур атак, предоставляемых вендором IDS;
– по возможности исключить установку и массовое использование администраторами сетей средств удаленного администрирования наподобие TeamViewer, RAdmin; в случае необходимости установки таких средств администрирования обеспечить протоколирование и хранение журналов сеансов администрирования, а также ограничить диапазон IP-адресов, с которых возможно удаленное подключение;
– составить единый список разрешенного к использованию программного обеспечения, своевременно актуализировать данный список, осуществлять контроль за соблюдением списка (возможна реализация техническими мерами через использование «белых

списков» штатными средствами ОС Windows либо сторонним специализированным ПО);

– исключить хранение в открытом виде паролей доступа к критичным информационным системам; в ряде известных специалистам ФинЦЕРТ случаев успешной реализации атак пароли хранились в текстовых файлах на рабочих столах администраторов и руководителей. По возможности организовать централизованное хранение паролей, а для задач администрирования использовать средства управления привилегиями (PAS, Privilege Access (Account) Security);
– в случаях выявления атак и неспособности самостоятельно справиться с ними и их последствиями рекомендуется привлекать специализированные экспертные организации (ФинЦЕРТ либо иные) для оказания помощи.

ЗАКЛЮЧЕНИЕ

Киберпреступники по-прежнему активны, и организациям кредитно-финансовой сферы необходимо уделять безопасности повышенное внимание. Крайне важно своевременно получать уведомления систем защиты и незамедлительно реагировать на них, а это требует постоянного мониторинга событий безопасности. Чтобы эффективно противостоять развивающейся киберпреступности, важно не скрывать произошедшие инциденты, а участвовать в обмене информацией об атаках внутри отрасли, чтобы вовремя узнавать об индикаторах компрометации и сообщать о них другим.

Spear-phishing кампании, вероятно, останутся основным путем распространения ВПО, однако в дальнейшем преступники будут разрабатывать и новые схемы атак на пользователей. Многоэтапные атаки, включая supply chain, также не потеряют актуальности. Поэтому организациям кредитно-финансовой сферы стоит уделить внимание как минимум двум направлениям работы. Во-первых, совместной работе со своими клиентами и партнерами в части повышения осведомленности сотрудников в области безопасности (security awareness) и обеспечения необходимого уровня защиты на их стороне. Это может достигаться различными путями, в том числе через проведение соответствующих тренингов по тематике информационной безопасности систем онлайн-банкинга на базе организации кредитно-финансовой сферы или предъявление конкретных требований к их защищенности.

Во-вторых, банки должны сосредоточиться на обеспечении безопасности во внутренней сети и внедрении средств защиты, которые позволят оперативно выявлять следы атак в инфраструктуре. Необходимо также использовать системы раннего предупреждения и детектирования атак в корпоративной сети, решения для поведенческого анализа файлов в безопасной среде (класса «песочница»). Однако обнаружить целевую атаку непосредственно в момент проникновения в локальную сеть сегодня практически невозможно. И в данном случае на помощь могут прийти средства глубокого анализа трафика, выявления в нем следов компрометации, инструменты и методики, детектирующие попытки закрепления в сети и использования легитимного ПО, ретроспективный анализ событий ИБ. В случае компрометации инфраструктуры избежать повторных инцидентов данного типа позволит проведение полноценного расследования с анализом инструментов злоумышленников и реакции используемых средств защиты.

Нужно внедрять системы защиты основных узлов и компьютерных систем, своевременно обновлять ПО – операционные системы, приложения, браузеры. Именно через старые версии офисного ПО и уязвимости в браузере происходит заражение вредоносным ПО, например Buhtrap. Атаки на веб-ресурсы входят в топ-3 по популярности в финансовом секторе (как и другие уязвимые сервисы, расположенные на периметре), поэтому повышению защиты веб-приложений следует уделять более пристальное внимание. В частности, необходим регулярный анализ их за-

щищенности, при этом наиболее эффективным способом проверки является метод «белого ящика», подразумевающий анализ исходного кода. В качестве превентивной меры рекомендуется использовать технологии всесторонней и непрерывной защиты веб-приложений, комбинирующие техники выявления аномалий, автоматической защиты от ранее неизвестных атак, обнаружения уязвимостей в исходном коде и блокировки атак на них и прочее. Это позволит предотвратить эксплуатацию уязвимостей, появляющихся в том числе при внесении изменений в код или добавлении новых функций.

При разработке приложений для мобильного и онлайн-банкинга необходимо уделять большее внимание балансу между их функциональностью и защищенностью. В частности, обеспечению безопасного хранения данных, устранению возможных ошибок в логике работы приложений. Учитывая, что большинство проблем возникают на этапе проектирования, банкам стоит задуматься о внедрении процесса безопасной разработки и приемки кода, повышении защищенности приложений на всех этапах их существования (в том числе и за счет регулярных аудитов).

Для того чтобы снизить риск атак на банкоматы, следует повысить физическую защиту сервисной зоны, так как доступ к встроенному компьютеру и точкам подключения периферийного оборудования – необходимое для эксплуатации большей части уязвимостей условие. Ведение регистрации и мониторинга событий безопасности позволит вовремя реагировать на возникающие угрозы. Помимо этого, важно регулярно проводить анализ защищенности банкоматов, чтобы своевременно выявлять и устранять существующие уязвимости. Анализ защищенности может дополнительно включать в себя исследование (реверс-инжиниринг) используемого ПО, в частности решений класса Application Control. Такие исследования позволяют выявить уязвимости нулевого дня и обеспечить защиту от новых, неизвестных ранее векторов атак.

Защита POS-терминалов, в свою очередь, требует разработки серьезного подхода к проблеме безопасности, включая проверку терминала в ходе регистрации и строгий мониторинг платежей.

Трейдинговые приложения пока не привлекли пристального внимания злоумышленников, но с учетом заинтересованности последних в легкой масштабируемости и быстрой монетизации атак необходимо повышать защищенность десктопных версий (в части шифрования передаваемых данных и ликвидации возможности выполнения произвольных команд) и мобильных – в части хранения данных. Следует выделять отдельный сегмент сети, в котором расположены торговые терминалы, и обеспечивать его защиту. Рекомендуется применять эффективные антивирусные средства для защиты конечных устройств и использовать технические решения, направленные на своевременное обнаружение подозрительной активности в сети. Важно регулярно проводить внешнее и внутреннее тестирование на проникновение, чтобы выявлять потенциальные векторы атак и оценивать эффективность принятых мер защиты. Для защиты веб-версий торговых платформ можно дополнительно использовать превентивные меры защиты, такие как межсетевой экран уровня приложений

(web application firewall, WAF), который обнаруживает и предотвращает известные атаки на веб-приложения, а также выявляет эксплуатацию уязвимостей нулевого дня.

Внедрение цикла безопасной разработки позволит избежать многих ошибок не только при разработке классических систем и приложений, но и в случае проектирования систем на базе технологии блокчейн. В частности, необходимо проводить детальный анализ архитектуры и конфигурации инфраструктуры информационной системы, анализировать исходный код информационной системы и смежных компонентов, выполнять регулярную независимую оценку безопасности как самой блокчейн-системы в целом, так и отдельных ее компонентов (смарт-контрактов, веб- и мобильных приложений).

Руководству организаций – клиентов учреждений кредитно-финансовой сферы на данный момент необходимо уделять внимание вопросу повышения грамотности персонала в области информационной безопасности. Компьютеры, которые работают с бухгалтерскими и банковскими системами, должны быть изолированы, а доступ по внешнюю сеть должен быть разрешен только по «белым спискам». Для защиты клиентов нужно использовать комплексные кросс-канальные решения, позволяющие без установки дополнительного программного обеспечения на устройства клиентов отслеживать и предупреждать атаки на стороне пользователей еще на этапе подготовки – за счет функций идентификации устройства, поведенческого анализа и выявления вредоносного ПО.

ПРИЛОЖЕНИЕ 1

GROUP-IB: АТАКИ НА ФИНАНСОВЫЕ ОРГАНИЗАЦИИ В РОССИИ И МИРЕ ЗА 2018 ГОД

МЕТОДОЛОГИЯ

Цель данного обзора – дать финансовым организациям представление о ландшафте угроз, наблюдавшихся в сфере информационной безопасности в 2018 году.

Описание и статистика угроз, а также оценка рынка основаны на данных из систем Group-IB Threat Intelligence, Group-IB Secure Bank и исследовании Лаборатории компьютерной криминалистики Group-IB.

Список рассматриваемых угроз не является исчерпывающим, описание технических деталей приведено исключительно для ознакомления с ними специалистов по информационной безопасности с целью предотвращения возникновения подобных инцидентов в дальнейшем и минимизации возможного ущерба.

ИТОГИ И ТРЕНДЫ 2018 ГОДА

По данным исследования киберинцидентов, проведенного командой реагирования Лаборатории компьютерной криминалистики Group-IB, в 2018 г. на финансовый сектор пришлось около 70% всей хакерской активности.

При этом эксперты Group-IB выявили несогласованность в работе внутренних подразделений, слабую проработку организационных процедур, необходимых для установления источника заражения, масштаба компрометации и локализации инцидента, а также недостаточную техническую подготовку персонала банков.

74% финансовых организаций оказались не готовы к кибератакам, из них:

- У 29% были обнаружены активные заражения вредоносными программами.
- В 52% случаев выявлены следы совершения атак в прошлом.
- Более 62% оказались не способны централизованно управлять своей сетью, что критично для скорости локализации инцидента и минимизации ущерба.
- 80% пострадавших организаций не имеют достаточной глубины «журналирования» событий протяженностью более месяца. Это затрудняет или делает невозможным восстановление ретроспективы атаки с этапа заражения до момента вывода денежных средств.
- Более 64% финансовых организаций, в которых работала команда по реагированию Group-IB, тратили на согласование работ

между подразделениями более четырех часов, тогда как для оперативной работы по горячим следам этот период не должен превышать одного часа.

Банк, инфраструктура которого оказалась взломанной, может не просто потерять денежные средства, но и стать угрозой для других игроков финансового рынка.

Финансово мотивированная хакерская группа, получая контроль над системами банка, заинтересована не только в выводе денег, но и в заражении максимального количества новых жертв. Для этой цели запускается вредоносная рассылка из скомпрометированной инфраструктуры по спискам компаний – партнеров банка. Такой вектор опасен тем, что письма отправляются из реального банка, то есть отправитель не подделан, а это повышает вероятность их открытия в банке-партнере.

В дополнение к финансовой мотивации наблюдаются атаки с целью создания негативного фона вокруг банка и нанесения урона репутации, тем самым провоцируя отток клиентов и партнеров, а затем уход банка с рынка.

Ниже представлен обзор ряда актуальных угроз, с которыми сталкивались пострадавшие компании в прошлом году, включая атаки с использованием вирусов-шифровальщиков, атаки на клиентов банков и на криптовалютные проекты.

АТАКИ С ИСПОЛЬЗОВАНИЕМ ВИРУСОВ-ШИФРОВАЛЬЩИКОВ

Несмотря на то, что наиболее крупномасштабные атаки с использованием вирусов-шифровальщиков, таких как WannaCry, NotPetya и Bad Rabbit, отгремели в 2017 г., этот вид вредоносного программного обеспечения остается одной из самых распространенных киберугроз и в 2018 г., пусть и потеряв в некотором смысле свой масштаб, но продолжая эволюционировать.

Современные вирусы-шифровальщики полностью исключают возможность расшифровки данных без соответствующего криптографического ключа, а целью их распространения становится не только запуск экземпляра вредоносной программы, но и изучение ИТ-инфраструктуры для дальнейшей компрометации и последующего шпионажа или кражи данных.

Как показывает опыт Лаборатории компьютерной криминалистики и исследования вредоносного кода Group-IB, наиболее популярным методом распространения программ-вымогателей является компрометация целевой системы путем подбора пароля к учетной записи с административными привилегиями и последующим доступом через протокол удаленного администрирования (RDP).

Многие системные администраторы оставляют RDP-порт (3389) на некоторых серверах открытым, чтобы облегчить себе работу и иметь доступ к указанным машинам в любое время и из любого места. При этом стандартная учетная запись администратора, которая, возможно, и не используется сотрудниками, не заблокирована, что значительно облегчает

злоумышленникам проведение атак по перебору пароля – логин им уже известен.

По данным Group-IB, посредством атак на RDP в 2018 г. наиболее часто распространялся вирус-шифровальщик GlobeImposter, о котором впервые стало известно в декабре 2017 года. Шифровальщик получал доступ к базам данных SQL, Outlook, PostgreSQL, 1C, а также к документам Word и таблицам Excel, которые были открыты в момент его запуска.

Однако более традиционные способы распространения, такие как фишинговые почтовые рассылки, также имеют место. В 2018 г. через них наиболее часто распространяли GandCrab, GlobeImposter, Hermes и Sigma.

АТАКИ НА КЛИЕНТОВ БАНКОВ

Атаки с использованием социальной инженерии

Согласно данным антифрод-подразделения Group-IB, более 80% хищений денежных средств у клиентов банков в России производится с использованием методов социальной инженерии, когда мошенники звонят жертвам и представляются сотрудниками банка, предлагая услуги, или представителями службы безопасности, которая якобы обнаружила подозрительную активность.

Злоумышленники получают от клиентов их личные данные и коды доступа, а затем выводят все средства со счетов. При этом вредоносное ПО либо не используется, либо «участвует» только на одном из этапов хищения.

В течение последнего года банки ежемесячно сталкивались в среднем с 3 тыс. атак с использованием социальной инженерии.

Один из актуальных примеров подобного рода мошенничества – работа черных брокеров, включающая следующие шаги:

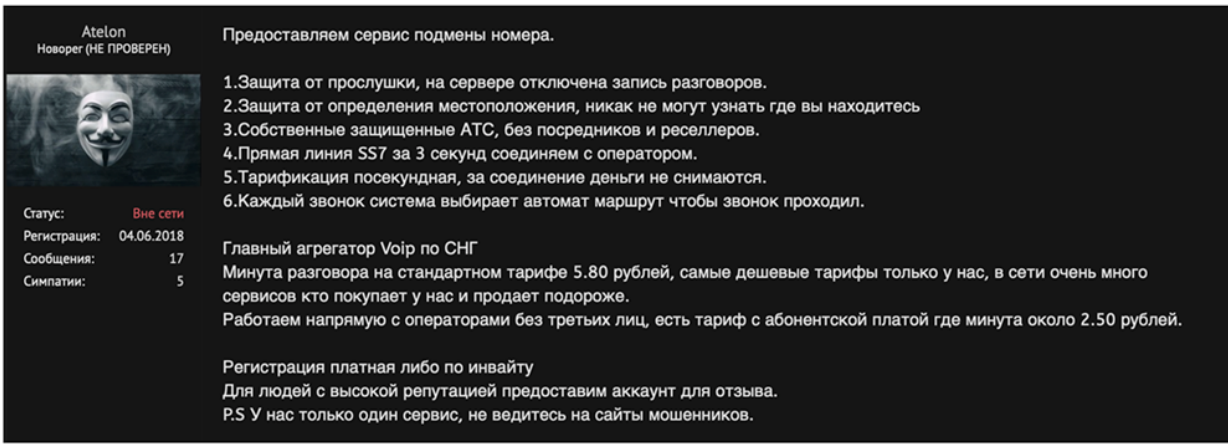
1. Мошенник звонит клиенту банка, представляясь сотрудником, и предлагает рассказать и показать, как можно выгодно инвестировать средства с использованием брокерских сервисов либо вывести уже вложенные средства и реинвестировать их.


Евгений :5 июн 2018 в 16:50
Приветствую! Со мной связались по телефону специалисты вашего банка или люди которые работают через вас , предложили помощь по возврату депозита с брокерского сайта Олимп-трейд. Попросили установить программу для удалённого управления рабочим столом AnyDesk. В этой программе их учётная запись предоставленна как "alfabank@ad". Далее просят поменять настройки в онлайн кабинете моего банка, якобы для того чтоб через ваш банк вернуть деньги с олимп-трейда на мою карту.
Подскажите пожалуйста, это новый вид разводы или вы действительно помогаете возвращать депозиты с брокерских сайтов?
Ответить

2. Для демонстрации возможностей они предлагают установить программу AnyDesk, являющуюся на самом деле инструментом для удаленного доступа к компьютеру.

3. Получив доступ, мошенник прямо с устройства пользователя списывает средства с его счета в онлайн-банке.

При звонке злоумышленники используют сервисы IP-телефонии с подменой номера, которые можно приобрести на хакерских ресурсах:

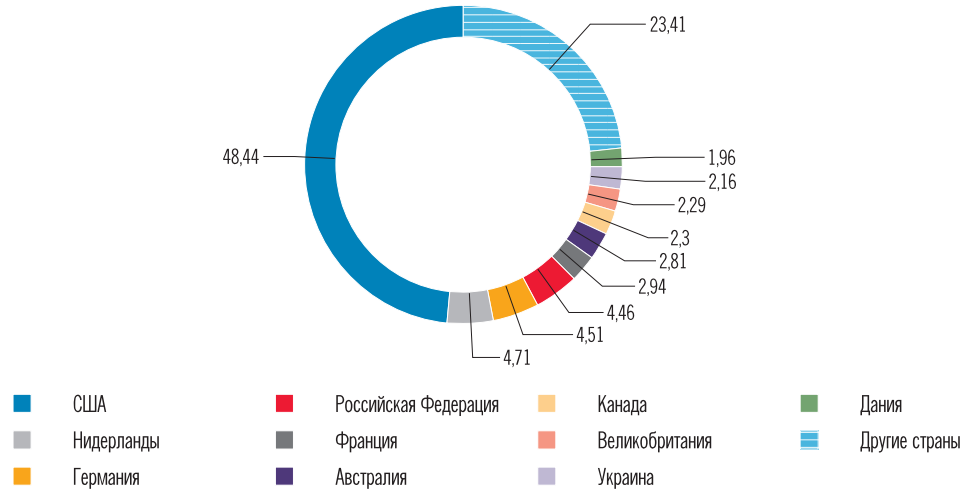


Атаки с помощью веб-фишинга

За 2018 г. системой Group-IB Threat Intelligence было обнаружено и проанализировано более 1,9 млн уникальных фишинговых ссылок, что на 85% больше, чем в 2017 году.

Более 26% из них приходится на финансовый сектор. Как и ожидалось, больше всего финансового фишинга относится к компаниям США (48% всех атак). Второе место занимают Нидерланды (4,7%), потом Германия (4,51%) и Россия (4,46%).

Рис. 1. Фишинг в финансовом секторе (топ-10 стран)



Основной способ привлечения пользователей на фишинговые страницы – это перенаправление посетителей со взломанных сайтов, а также попадание мошеннических ресурсов в поисковую выдачу. В России, в отличие от многих других стран, под большую часть фишинговых сайтов регистрируется отдельное доменное имя.

Фишеры, занимающиеся массовыми атаками, используют специальные фишинг-наборы (phishing kits). За прошедший период система Group-IB Threat Intelligence собрала более 18 237 таких уникальных наборов и проанализировала их конфигурационные файлы. В подавляющем большинстве случаев скомпрометированные данные отправлялись на адрес электронной почты.

Атаки с использованием JS-снифферов

В последние два года наблюдается растущая угроза снифферов – типа вредоносного кода, внедряемого злоумышленниками в скрипт сайта жертвы для перехвата вводимых пользователем данных: номеров банковских карт, имен, адресов, логинов, паролей и так далее. Полученные платежные данные злоумышленники перепродают или используют сами для покупки и перепродажи ценных товаров.

По результатам исследования, проведенного Group-IB в начале 2019 г., выявлено 38 различных семейств снифферов, восемь из них обнаружены впервые.

TokenLogin	Март 2016	Illum	Конец 2016	MagentoName	Декабрь 2017
TokenMSN	Середина 2016	WebRank	Конец 2016	ImageID	Конец 2017
G-Analytics	Сентябрь 2016	ReactGet	Июнь 2017	GetBilling	Начало 2018
PreMage	Ноябрь 2016	PostEval	Середина 2017	Qoogle	Апрель 2018
FakeCDN	Ноябрь 2016	CoffeMokko	Сентябрь 2017	GMO	Май 2018

Список семейств JS-sniffer, проанализированных в этом отчете: 15 из 38, обнаруженных командой Group-IB

Специалисты проанализировали 2440 зараженных онлайн-магазинов США, Великобритании, Германии и других крупных развитых стран, принимающих к оплате банковские карты. Суммарное суточное количество посетителей всех зараженных сайтов – более 1,5 млн человек.

При заражении сайта в цепочку пострадавших оказываются вовлеченными все стороны – конечные пользователи, платежные системы, банки и крупные компании, торгующие своими товарами и услугами через сеть Интернет.

Для платежных систем и банков-эквайрингов угроза снифферов несет риски незаконного использования бренда на фишинговых страницах, последующее снижение доверия пользователей к банку и соответствующий репутационный ущерб.

Для банков-эмитентов в дополнение к вышеперечисленному это может повлечь компрометацию данных карт клиентов, операционные издержки на расследование запросов клиентов и возмещение ущерба в случае успешной атаки.

Архитектура снифферов

С точки зрения архитектуры каждый сниффер имеет клиентскую и серверную части.

1. Клиентская часть сниффера отвечает за первоначальный сбор данных, осуществляемый разными способами:

- по жестко записанному списку имен полей платежных форм;
- по списку регулярных выражений, определяющих интересные снифферу поля;
- по списку базовых HTML-элементов, используемых в платежной форме.

2. Серверная часть сниффера – приложение, с которым работает оператор сниффера: выполняемые серверной частью функции зависят от того, насколько точно клиентская часть сниффера определяет тип украденных данных. Если данные передаются в необработанном виде, значит, приведение номера карты, CVV, телефона, электронной почты и имени владельца к единому виду происходит уже в административной панели.

Обработка данных в административной панели – более удобный вариант, так как внести изменения в код административной панели легче, чем изменить код сниффера, уже внедренного на сайт онлайн-магазина.

Тем не менее многие семейства снифферов используют уникальные варианты для каждой отдельной платежной системы, что требует модификации и тестирования скрипта перед каждым заражением.

Как работают снифферы

1. Получение доступа к сайту одним из трех возможных вариантов:
   - Получение логина и пароля к административной панели с использованием вредоносных программ, крадущих пароли.
   - Поиск уязвимых сайтов (эксплойты популярных CMS, известные уязвимости поставщиков услуг). Используя эксплойты, злоумышленник загружает веб-шелл и получает доступ к изменению файлов сайта.
   - Покупка доступа к сайту у другой группы злоумышленников.

2. Разработка сниффера или покупка/аренда готового варианта на теневом форуме.

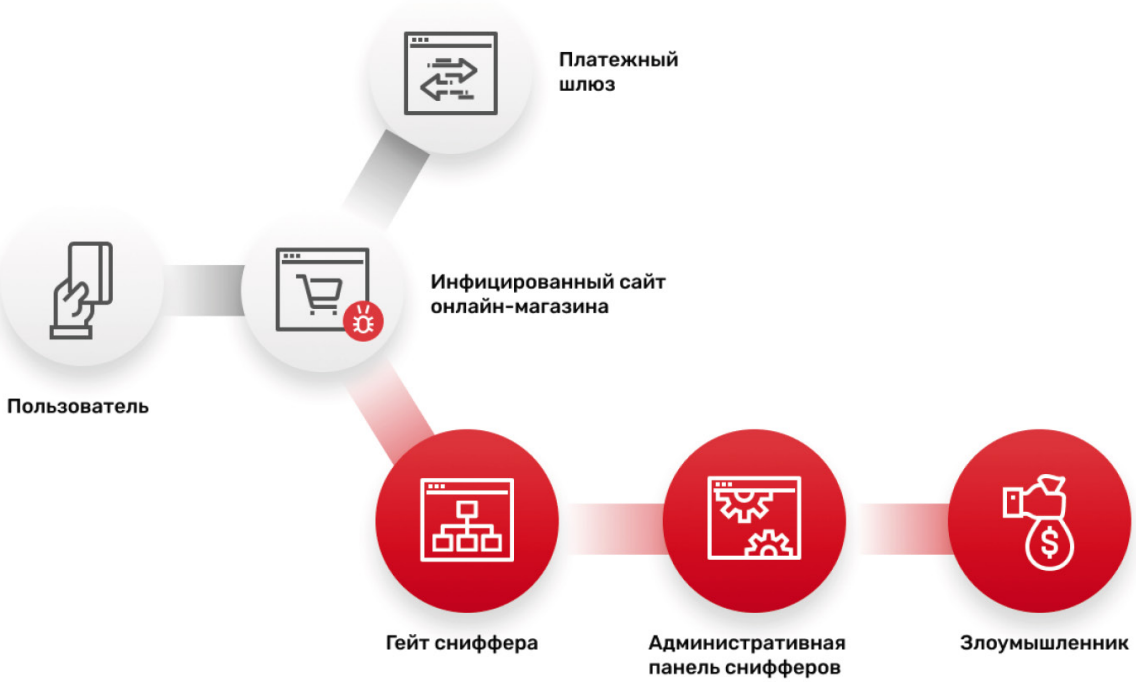
3. Установка сниффера: установленный через панель управления или веб-шелл сниффер собирает информацию и отправляет ее на хост, управляемый злоумышленником. Некоторые снифферы используют техники, позволяющие оставаться незамеченными при ручной проверке: добавление в легитимную библиотеку скриптов или механизм приостановки активности сниффера в момент использования консоли разработчика (например, Chrome DevTools или Firefox Browser Toolbox).

Монетизация:

- Продажа данных кардерам и получение от 1 до 5 долл. США с каждый карты. Этот способ самый простой – для его реализации достаточно иметь контакты проверенных скупщиков.

- Оплата чужими банковскими картами товаров, которые легко перепродать: гаджетов, электроники, бытовой техники, предметов интерьера, одежды и обуви.

Собранные платежные данные и персональную информацию жертвы отправляют на сервер злоумышленников – гейт. Для усложнения задачи обнаружения конечного сервера злоумышленников в цепочке передачи данных со сниффера может быть использовано несколько уровней гейтов, расположенных на разных серверах или взломанных сайтах. Однако в некоторых случаях административная панель расположена на том же хосте, что и гейт для сбора украденных данных.



Конечный сервер злоумышленников, предназначенный для отслеживания активности снифферов и экспорта украденных данных, может представлять собой как полноценную административную панель, так и сервер для размещения инструментов администрирования баз данных. К примеру, функции административной панели могут выполнять такие инструменты, как Adminer или phpMyAdmin.

Способы заражения

Злоумышленники могут заражать сайты и внедрять вредоносный код разными способами:

1. При помощи уязвимостей CMS, разработанных специально для онлайн-магазинов, – Magento, OpenCart и других:

- загрузка веб-шелла на сайт посредством эксплуатации уязвимости с последующей модификацией файлов сайта;
- внедрение кода сниффера через эксплуатацию уязвимости, позволяющей добавить код злоумышленника в один из блоков кода сайта, к примеру в футер (нижний сквозной блок страниц сайта).

2. Через получение доступа к административной панели сайта с возможностью редактирования файлов. Компрометация логина и пароля может осуществляться несколькими методами:

- использование стилеров – программ, позволяющих извлекать пароли, сохраненные в браузере;
- использование вредоносных программ для перехвата вводимых данных (в том числе логина и пароля);
- брутфорс – метод перебора паролей.

3. Путем взлома сторонних сервисов, скрипты которых работают на целевом сайте:

- внедрение вредоносного кода через код скриптов сайтов, предоставляющих услуги онлайн-магазинам (чаты клиентской поддержки, системы аналитики и статистики);
- взлом аккаунтов CDN-сервисов с возможностью модификации скриптов, подгружающихся из CDN на целевые сайты.

Атаки через поставщиков

Преступная группа, стоящая за использованием семейства снифферов WebRank, зачастую осуществляла атаки через поставщиков услуг. К примеру, взломав систему веб-аналитики, злоумышленники внедряли в ее скрипт код сниффера. Данный скрипт, подгружаемый многими сайтами, вместе с собой подгружал и сниффер банковских карт.

Другой пример – атака на Feedify, сервис для push-уведомлений в режиме реального времени. Внедрив код сниффера в код файла, преступная группа автоматически подгружала сниффер всем клиентам компании Feedify, на сайты которых подгружался скрипт feedbackembad-min-1.0.js. Сниффер был впервые добавлен в код Feedify 17 августа, а 11 сентября обнаружен и удален. Однако злоумышленники вновь провели заражение 12 сентября.

Атаки через сторонних поставщиков доказали свою эффективность: более 60% из 300 сайтов, подгружающих скрипт Feedify, относятся к ecommerce-сайтам, на которых совершаются операции по онлайн-оплате товаров и услуг. Поэтому они полностью соответствуют задачам сниффера семейства WebRank.

Универсальные снифферы

К универсальным снифферам можно отнести те семейства, которые настроены на кражу данных из разных платежных систем и не требуют доработки под определенную платежную систему.

Снифферы семейств G-Analitycs и WebRank настроены похищать все содержимое элементов HTML определенного типа. Это означает, что парсинг украденных данных происходит в административной панели этих снифферов, то есть на стороне сервера.

- Снифферы семейства WebRank обращаются ко всем объектам типа «text», «a», «button», «input», «submit» и «form» и добавляют специальные обработчики событий, связанных с этими элементами.

- Снифферы семейства G-Analytics осуществляют поиск всех элементов следующих типов на странице оплаты: «input», «select», «textarea», «checkbox». Если в результате этого поиска обнаруживаются данные, похожие на номер кредитной карты, сниффер отправит эти данные на сервер злоумышленников.

Снифферы для определенных CMS

Большая часть обнаруженных снифферов нацелена на платежные формы определенных CMS, то есть сниффер осуществляет поиск определенных полей, содержащих платежную информацию, и список таких полей жестко записан в коде сниффера.

Следующие снифферы осуществляют поиск стандартных полей платежной формы CMS Magento:

- PreMage;
- MagentoName;
- FakeCDN;
- Qoogle.

Сниффер GetBilling также нацелен на платежную форму CMS Magento, но вместо поиска по списку полей он осуществляет поиск форм по их имени.

Сниффер семейства PostEval нацелен на платежные формы сайтов, работающих под управлением CMS OpenCart. Для поиска данных сниффер использует жестко закодированные имена полей.

Сниффер как сервис

При анализе теневых форумов, предназначенных для общения киберпреступников, было обнаружено большое количество сервисов, предлагающих своим клиентам полностью готовое решение, в которое входят:

- сниффер или утилита для генерации снифферов;
- административная панель для обработки данных и отслеживания активности снифферов;
- инструкции по заражению сайтов онлайн-магазинов;
- готовые эксплойты для заражения сайтов;
- вспомогательные утилиты для поиска уязвимостей и массовых заражений сайтов.

При анализе обнаруженных семейств снифферов было установлено, что в некоторых случаях домены, использованные для хранения кода сниффера или для сбора украденной информации, были зарегистрированы разными пользователями. Код был модифицирован, применялись разные способы обфускации («запутывания» кода) и техники сокрытия вредоносной активности. Эти факторы указывают на то, что семейство снифферов используется разными преступными группами, то есть поставляется как сервис.

В других случаях прослеживалась четкая специфика деятельности определенной преступной группы, что может означать независимость от сторонних разработчиков и использование только собственных разработок. Таким образом, эти преступные группы должны иметь как минимум

одного человека, имеющего навык веб-разработки и знакомого с такими языками, как HTML, JavaScript и PHP.

КАРДИНГ

Рынок кардинга можно поделить на два основных сегмента: продажа текстовых данных о картах (номер, дата истечения, имя держателя, адрес, CVV) и дампов (содержимое магнитных полос карт).

Текстовые данные собираются с помощью фишинговых сайтов, банковских троянов для ПК, Android, банкоматов, а также в результате взломов ecommerce-сайтов. Дампы получают через скимминговые устройства, а также с использованием троянов для компьютеров, к которым подключены POS-терминалы.

Большая часть скомпрометированных карт продается на специализированных «кардшопах», куда в среднем каждый месяц загружается 686 тыс. текстовых данных карт и 1,1 млн дампов.

По данным Group-IB Threat Intelligence, более 62% продаваемых данных относится к дампам, что делает POS-угрозы основным методом компрометации банковских карт.

Суммарный объем рынка кардинга за прошедший период оценивается в 663,4 млн долл. США. При этом текстовая информация о банковских картах продавалась значительно дешевле дампов, составляя лишь 17% от общей суммы (95,6 млн долл. США против 567,8 млн долл. США).

	Текстовые данные	**Дампы**	**Всего**
Общее количество	10 218 489	16 927 777	27 146 266
Размер рынка, долл. США	95 590 424	567 791 443	663 381 867
Минимальная цена, долл. США	0,75	0,5	
Максимальная цена, долл. США	99,99	295	
Средняя цена, долл. США	9,35	33,54	
Медиана, долл. США	8	25	

АТАКИ НА КРИПТОВАЛЮТНЫЕ ПРОЕКТЫ

Ландшафт угроз для криптовалютного рынка непрерывно изменяется, и в 2018 г. мы видели появление новых схем, а также адаптацию старых. Наибольший интерес представляют целенаправленные атаки.

МАНИПУЛЯЦИИ КУРСАМИ КРИПТОВАЛЮТ

Большинство мошеннических схем пришли на криптовалютный рынок от мошенников, которые действуют на традиционных рынках.

Еще в 2015 г. мы рассказывали о том, как *группа Corkow взломала банк* и, используя его брокерские счета, повлияла на обменный курс рубля. Аналогичное мошенничество совершили неустановленные хакеры в начале 2018 года. Подготовка атаки заняла более двух месяцев.

Тактика действия атакующих на криптовалютном рынке была следующей:

1. В январе 2018 г. неизвестная группа хакеров создала фишинговый домен, название которого созвучно с крупнейшей китайской криптобиржей Binance.

2. Началась рассылка ссылок на фишинговый ресурс трейдерам этой криптобиржи с целью получения их логинов и паролей.

3. Получив логины и пароли, атакующие смогли создать API-ключи, которые позволяют автоматизировать работу с биржей.

4. 7 марта 2018 г. в течение двух минут атакующие автоматически, используя созданные ранее API-ключи скомпрометированных трейдеров, разместили множество заявок на покупку малоизвестной криптовалюты Viacoin.

5. Заявки на покупку привели к тому, что через 30 минут курс Viacoin подскочил на 143% – с 2,80 до 6,79 долл. США, по данным coinmarketcap.com.

6. После того как курс Viacoin вырос, атакующие начали продавать их за Bitcoin с 31 заранее подготовленного аккаунта.

7. По окончании торгов были отправлены запросы на вывод средств.

Рис. 2. Viacoin Charts

Целевой взлом криптобирж

В 2017 и 2018 гг. происходил рост интереса хакеров к криптобиржам. Всего было ограблено восемь криптовалютных бирж. Минимум пять из них связывают с атакой северокорейских хакеров из группппы Lazarus, чьи жертвы преимущественно находятся в Южной Корее. Биржа YouBit (бывшая Yapizon) после второй атаки потеряла 17% своих активов и обанкротилась.

Всего за период было похищено 780 млн долл. США (54% от общей суммы – с японской биржи Coincheck).

Дата	Название проекта	Страна	Похищено в криптовалюте	Похищено, млн долл. США
Январь 2018	Coincheck	Япония	523 млн NEM	534
Февраль 2018	Bitgrail	Италия	17 млн NANO	170
Июнь 2018	Buthumb	Южная Корея	-	32
	Coinrail		11 разных криптовалют	37
	Bancor	-	-	23
Сентябрь 2018	Zaif	Япония	5 966 биткойнов	60
Март 2019	DragonEx	Сингапур	-	-
	Bithumb	Южная Корея	3 млн EOS 20 млн XRP	18,5
Май 2019	BitoPro	-	7 млн XRP	2,17
	Binance	Гонконг	7 000 биткойнов	40,5

Основной вектор проникновения в корпоративные сети криптобирж – целевой фишинг. Для этого злоумышленники отправляют:

- поддельные резюме, например с темой «Engineering Manager for Crypto Currency job»;
- «Investment Proposal.doc» от имени юридических компаний;
- поддельные соглашения «AGREEMENT.docx» от имени криптобирж, например южнокорейской EyaLabs и Falcon Coin.

Как правило, вредоносные вложения – это документы с макросами или уязвимостями. В случае запуска вредоносных файлов на компьютеры жертв устанавливаются средства удаленного управления (RAT).

Организуя скрытые каналы между зараженными устройствами и серверами управления, им удается исследовать локальную сеть, чтобы найти рабочие места или серверы, где осуществляется работа с приватными кошельками криптобирж.

РЕКОМЕНДАЦИИ GROUP-IB

Для того чтобы компании не становились жертвами киберпреступников, эксперты Group-IB рекомендуют правильно выстраивать систему проактивной защиты, исходя из актуальных киберугроз.

1. Необходимо использовать системы раннего предупреждения и детектирования атак в корпоративной сети, решения для поведенческого анализа файлов в безопасной среде (класса «песочница»).

2. Для защиты клиентов нужно использовать комплексные кросс-канальные решения, позволяющие без установки дополнительного программного обеспечения на устройства клиентов отслеживать и предупреждать атаки на стороне пользователей еще на этапе подготовки – за счет функций идентификации устройства, поведенческого анализа и выявления вредоносного ПО.

3. Компьютеры, которые работают с бухгалтерскими и банковскими системами, должны быть изолированы, а доступ по внешнюю сеть должен быть разрешен только по «белым спискам» (white lists).

4. Необходимо внедрять системы защиты основных узлов и компьютерных систем, своевременно обновлять ПО – операционные системы, приложения, браузеры. Именно через старые версии офисного ПО и уязвимости в браузере происходит заражение программой Buhtrap.

5. Кроме того, сотрудники, попадающие в «группу риска» (бухгалтеры, системные администраторы, секретари), в обязательном порядке должны проходить тренинги по информационной безопасности, а всю IT-инфраструктуру компании два раза в год необходимо проверять в ходе «боевых учений».

6. Для того чтобы знать о готовящихся атаках заранее, необходимо выходить за пределы собственного периметра и получать информацию об угрозах, преступных группах, их тактике и используемых инструментах. Лучше всего это позволяет сделать система предупреждения киберугроз Threat Intelligence (киберразведка).

ПРИЛОЖЕНИЕ 2

POSITIVE TECHNOLOGIES: ЗАЩИЩЕННОСТЬ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ, ИТОГИ 2018 ГОДА. ОЦЕНКА

МЕТОДОЛОГИЯ

Отчет основан на данных, полученных в ходе выполненных компанией Positive Technologies в течение 2018 г. работ по анализу защищенности корпоративной инфраструктуры финансовых организаций, банкоматов, мобильных и онлайн-банков, торговых платформ. Также в выборку вошли итоги работ экспертного центра безопасности Positive Technologies (PT Expert Security Center) по расследованию киберинцидентов и ретроспективному анализу событий безопасности в инфраструктуре компаний и отслеживанию активности APT-группировок, действующих в финансовом секторе, за 2018 год. При подготовке материала использована общедоступная информация об актуальных угрозах информационной безопасности и данные аналитических отчетов компании Positive Technologies за 2017–2018 годы.

ОБЩИЕ ТЕНДЕНЦИИ 2018 ГОДА

Кредитно-финансовые организации входят в число наиболее атакуемых киберпреступниками. В течение 2018 г. общее число атак росло при снижении количества успешных (снизился финансовый ущерб от них).

В большинстве атак использовалось вредоносное ПО, часто доставляемое с использованием социальной инженерии, в частности – фишинга. Во внутренней сети уровень их защищенности мало чем отличается от компаний из других отраслей и достаточно низок. Это позволяет злоумышленникам беспрепятственно перемещаться по сети, получать доступ к критически важным системам, управлению банкоматами и карточному процессингу.

Исследования защищенности банкоматов и платежных терминалов показывают, что используемые механизмы безопасности недостаточно эффективны. Выявленные уязвимости и недостатки механизмов защиты позволяют похитить деньги или перехватить данные банковских карт. В 2018 г. были зафиксированы преимущественно атаки типа blackbox.

Главная позитивная тенденция в безопасности финансовых приложений в 2018 г. – сокращение доли уязвимостей высокого уровня риска в онлайн-банках. Однако в целом их защищенность остается низкой: кража денежных средств в 2018 г. была возможна в 54% онлайн-банков (что несколько выше показателя 2017 г., составившего 50%), в отдельных случа-

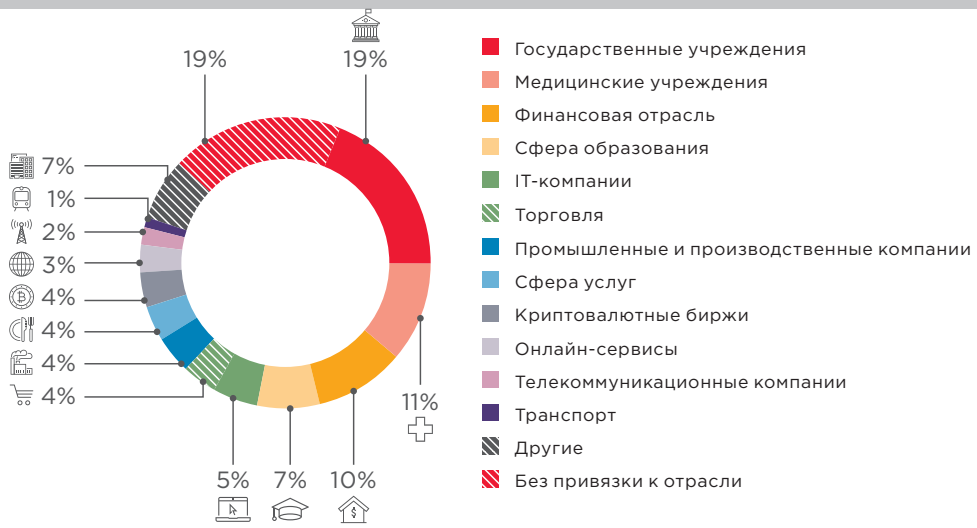
ях уязвимости позволяли развивать атаку до проникновения в корпоративную инфраструктуру.

Преступники могут наметить себе и новые объекты атак, которые пока не привлекают их внимания. Например, большое число уязвимостей выявляется в торговых платформах, используемых в финансовых организациях. Атаки на них еще не распространены, но имеют шансы превратиться в новый тренд в ближайшее время и потенциально могут вызвать изменение цен на бирже и привести к потере денег.

Краткая статистика: инциденты и методы атак

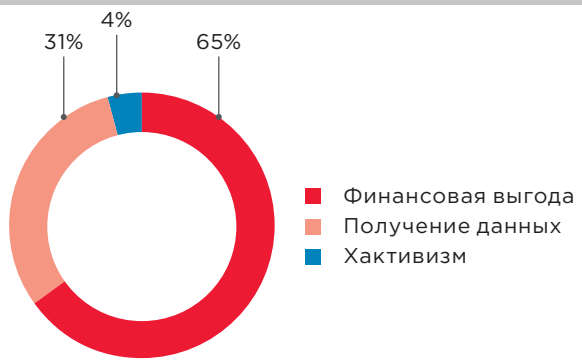
По итогам 2017 и 2018 гг. кредитно-финансовые организации являются наиболее атакуемыми: они входят в топ-3 по общему количеству атак.

Рис. 1. Категории жертв среди юридических лиц



Главный мотив злоумышленников – получение финансовой выгоды (65% инцидентов в 2018 г. и 92% – в 2017 г.). Доля инцидентов, нацеленных на получение информации о платежных картах, персональных данных, учетных данных пользователей для доступа к личным кабинетам, с 2017 по 2018 г. увеличилась с 8 до 31%.

Рис. 2. Мотивы атак на организации кредитно-финансовой сферы



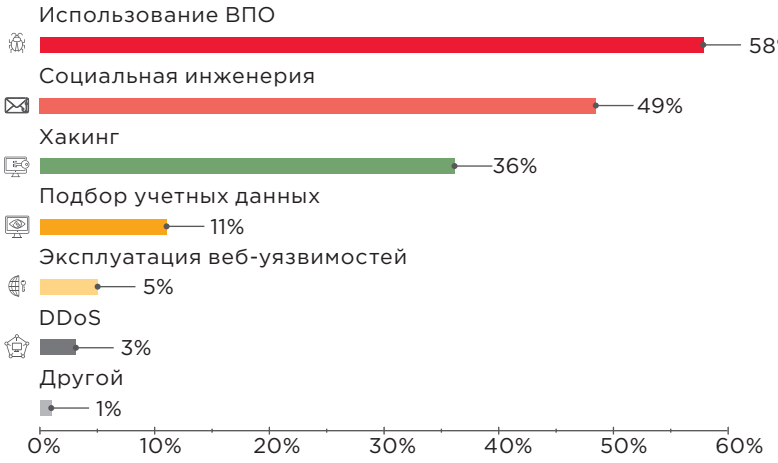
Среди методов атак по итогам 2018 г. лидируют использование ВПО (58%), социальная инженерия (49%), хакинг (36%), подбор учетных данных (11%) и эксплуатация веб-уязвимостей (5%). В целом это повторяет тенденции 2017 года. Растет доля атак, в ходе которых используется вредоносное ПО. В 2017 г. мы отмечали, что ВПО применялось в 48% случаев, в 2018 г. доля таких атак составила 58%. Этому способствует то, что ВПО с каждым годом становится более доступным и, соответственно, снижается порог входа в киберпреступный бизнес.

В финансовых организациях система защиты, как правило, хорошо организована, поэтому главным вектором проникновения в инфраструктуру остается социальная инженерия, применяемая в 49% атак. Фишинг – самый эффективный способ доставки вредоносного ПО. 90% актуальных на сегодня APT-группировок используют его на этапе проникновения.

Поиск и эксплуатация уязвимостей в публично доступных сервисах (хакинг) применяются в 36% атак на финансовые организации, а подбор учетных данных и эксплуатация веб-уязвимостей – в 11 и 5% атак соответственно. Под угрозой в этом случае оказываются скорее банки среднего звена, не всегда готовые вкладывать крупные бюджеты в обеспечение собственной безопасности. Небольшие банки могут оказаться промежуточным звеном атаки: например, с компьютеров их сотрудников могут рассылаться фишинговые письма в адрес их коллег из более крупных банков.

Нередко злоумышленники комбинируют эти методы в ходе атаки.

Рис. 3. Методы атак на организации кредитно-финансового сектора



Резюме: вредоносное ПО и социальная инженерия укрепляют свои позиции

Вредоносное ПО будет и дальше широко применяться в атаках на финансовые организации. Рынок киберуслуг и ВПО активно развивается – все больше группировок предпочитают не разрабатывать собственное ПО, а покупать готовое. Одни и те же программы, вероятно, будут использоваться разными группами киберпреступников, что существенно усложнит атрибуцию.

В тренде у преступников использование уязвимостей в продуктах Microsoft, причем все чаще применяются вновь опубликованные эксплойты (окно между появлением новой технологии и принятием ее на вооружение может исчисляться часами).

Преступники будут искать новые пути распространения вредоносного ПО и совершенствовать старые. Социальная инженерия, вероятно, останется основным путем распространения, однако рост осведомленности о различных способах мошенничества заставит преступников разрабатывать новые схемы обмана пользователей. Многоэтапные атаки (через supply chain) также не потеряют актуальности.

ПОРТРЕТ ЗЛОУМЫШЛЕННИКА

Общий тренд: мотив, вектор атаки, результативность

Ключевой мотив злоумышленников, атакующих организации кредитно-финансового сектора, – прямая финансовая выгода. И даже атаки, нацеленные на получение информации о платежных картах, персональных данных, учетных данных пользователей для доступа к личным кабинетам и так далее, в дальнейшем могут быть монетизированы за счет последующей кражи денег со счетов либо их перепродажи на теневом рынке. На долю такого типа информации приходится до 83% всех продаваемых и покупаемых в дарквебе данных.

Основной вектор, используемый атакующими для доступа в корпоративную сеть кредитно-финансовых организаций, – фишинг. С каждым годом качество составления фишинговых сообщений улучшается. А на стороне атакующих появляются новые игроки. Так, во втором полугодии 2018 г., помимо известных APT-группировок, атакующих финансовый сектор, была обнаружена новая. Злоумышленники также рассылали документы с макросами, которые загружали утилиты, предоставляющие удаленный доступ к зараженному компьютеру.

Ключевые группировки: хорошо известные и новички

Cobalt

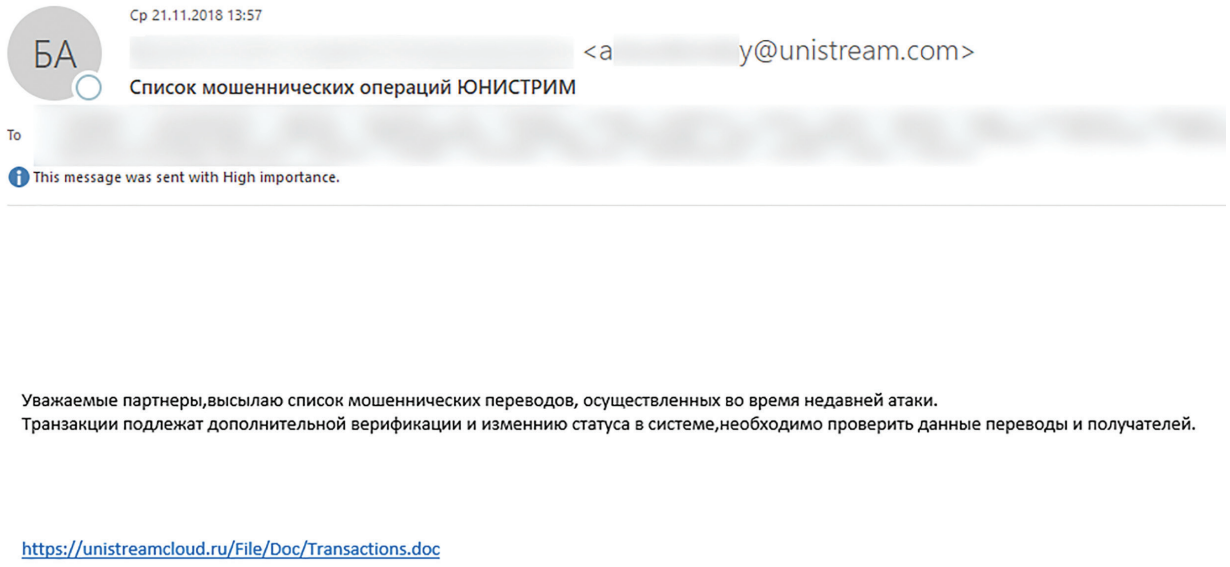
Группа Cobalt за 2018 г. выполнила 61 рассылку по кредитно-финансовым организациям в России и странах СНГ. Из них на I, II, III и IV кварталы пришлось по 12, 12, 24 и 13 рассылок соответственно[7]. Главная цель группы – кража денежных средств со счетов финансовых организаций. Основные используемые методы – это компрометация банкоматной сети либо подделка платежных документов. Для доставки ВПО в корпоративную сеть группа пользуется фишинговыми письмами: для каждой рассылки подготавливался отдельный домен, с которого рассылались письма с заранее подготовленным убедительным содержанием. В некоторых случаях с них же загружалась полезная нагрузка.

Большую часть года группировка использовала JS-бэкдор, с августа перешла на распространение вредоносного ПО CobInt, но в октябре

[7] *По данным PT Expert Security Center.*

вернулась к использованию JS-бэкдора. Фишинговые рассылки в августе и начале сентября проводились с поддельных доменных адресов, якобы принадлежавших платежной системе Interkassa, а также банкам BBVA Compass Bancshares, Европейскому центральному банку, Unibank, АЛЬФА-БАНКу, Райффайзенбанку. В течение IV квартала рассылка проводилась от лица взломанных банков – например, от имени Unistream. Примечательно, что группировка провела вредоносную рассылку менее чем через двое суток с момента публикации информации об уязвимости нулевого дня CVE-2018-15982 (в течение 34 часов)[8].

Рис. 4. Пример фишингового письма, рассылаемого группировкой Cobalt



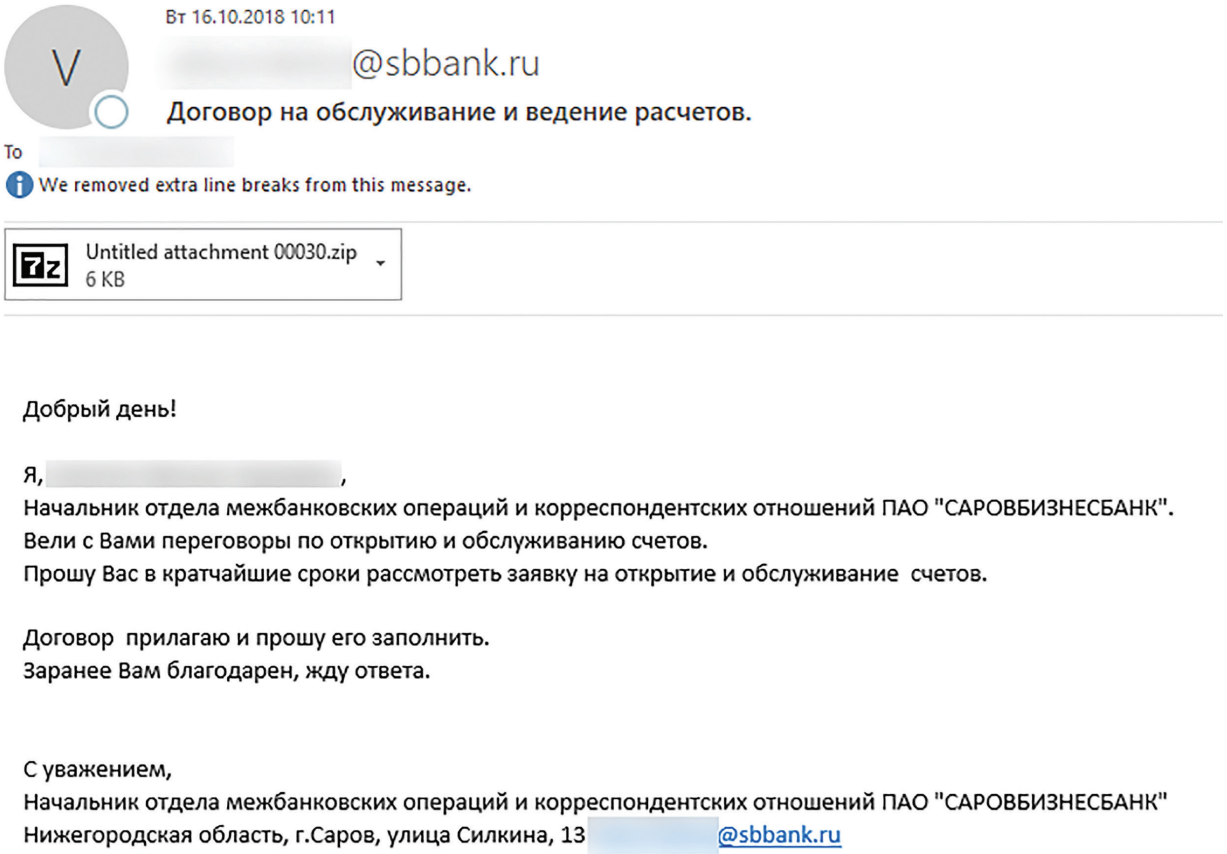
Silence

В 2018 г. группировка Silence провела 7 атак (в II квартале – 3, в IV – 4)[9]. Группа не очень разнообразно подходит к составлению фишинговых писем: разница между рассылками 2017 и 2018 гг. минимальна.

[8] *По данным PT Expert Security Center.*

[9] *По данным PT Expert Security Center.*

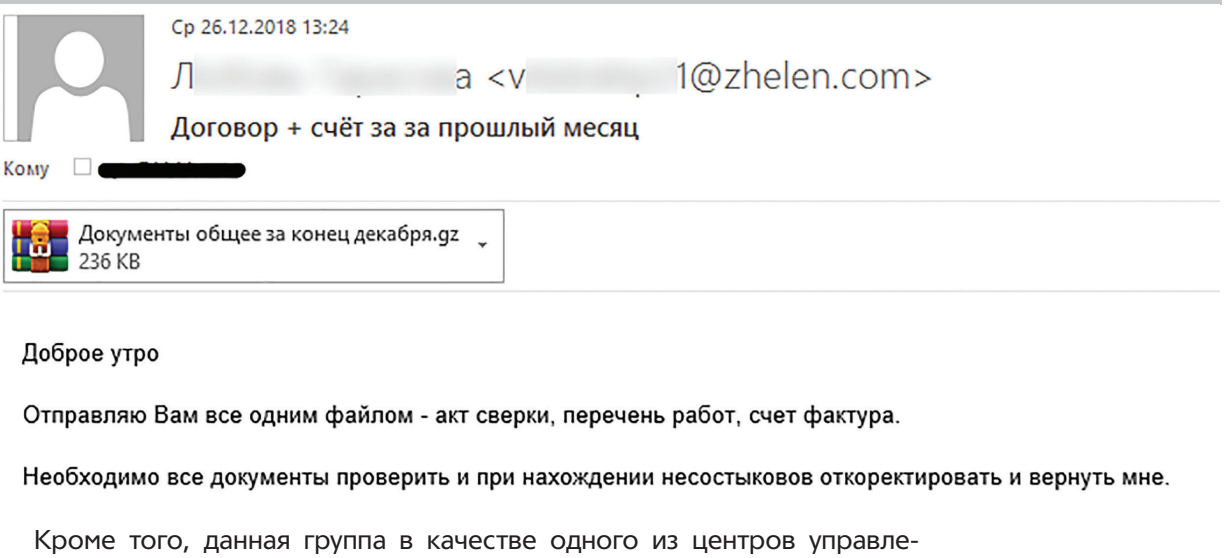
Рис. 5. Пример фишингового письма, рассылаемого группировкой Silence



RTM

Группа RTM за 2018 г. провела 59 рассылок, в том числе нацеленных на финансовые учреждения. В I квартале группировка выполнила 5 из них, в II – 14, в III – 17 и в IV – 23 рассылки. Атакуя, группа пытается получить доступ к финансовым счетам организаций и уже с них производит кражу денег. Для получения доступа в корпоративную сеть используются фишинговые рассылки. С начала своей активности группа придерживается неизменного их формата.

Рис. 6. Пример фишингового письма, рассылаемого группировкой RTM



Кроме того, данная группа в качестве одного из центров управления использовала домены в зоне.bit[10]. Это специальная зона, созданная на базе технологии блокчейн Namecoin: защищенная от цензуры и принудительного изъятия доменов альтернатива традиционным регистраторам DNS. Особенности архитектуры блокчейна позволили специалистам PT Expert Security Center разработать алгоритм отслеживания регистрации новых доменов группировки RTM (или смену их IP-адресов). Это позволило уведомлять кредитно-финансовые организации и комьюнити о новых управляющих серверах с задержкой в минуты с начала (иногда и до) их использования злоумышленниками.

Новые игроки

Во второй половине 2018 г. была выявлена новая группировка, атакующая финансовый сектор. Злоумышленники рассылали вредоносные документы с макросами якобы от лица ФинЦЕРТ. При исполнении макроса на компьютер загружалась полезная нагрузка – *Metasploit stager*.

Также была зафиксирована рассылка, которая проводилась через скомпрометированную учетную запись сотрудника компании «Альфа Капитал». При анализе рассылаемого документа был обнаружен сценарий на JavaScript, который использовала группа Treasure Hunters, однако в него была добавлена функция запуска Metasploit stager. В обоих случаях письма были очень хорошо подготовлены.

[10] *В последние годы его начали использовать операторы таких ботнетов, как Dimnie, Shifu, RTM и Gandcrab, для управления адресами C&C-серверов.*

Рис. 7. Пример фишингового письма, рассылаемого новой группировкой, атаковавшей кредитно-финансовый сектор

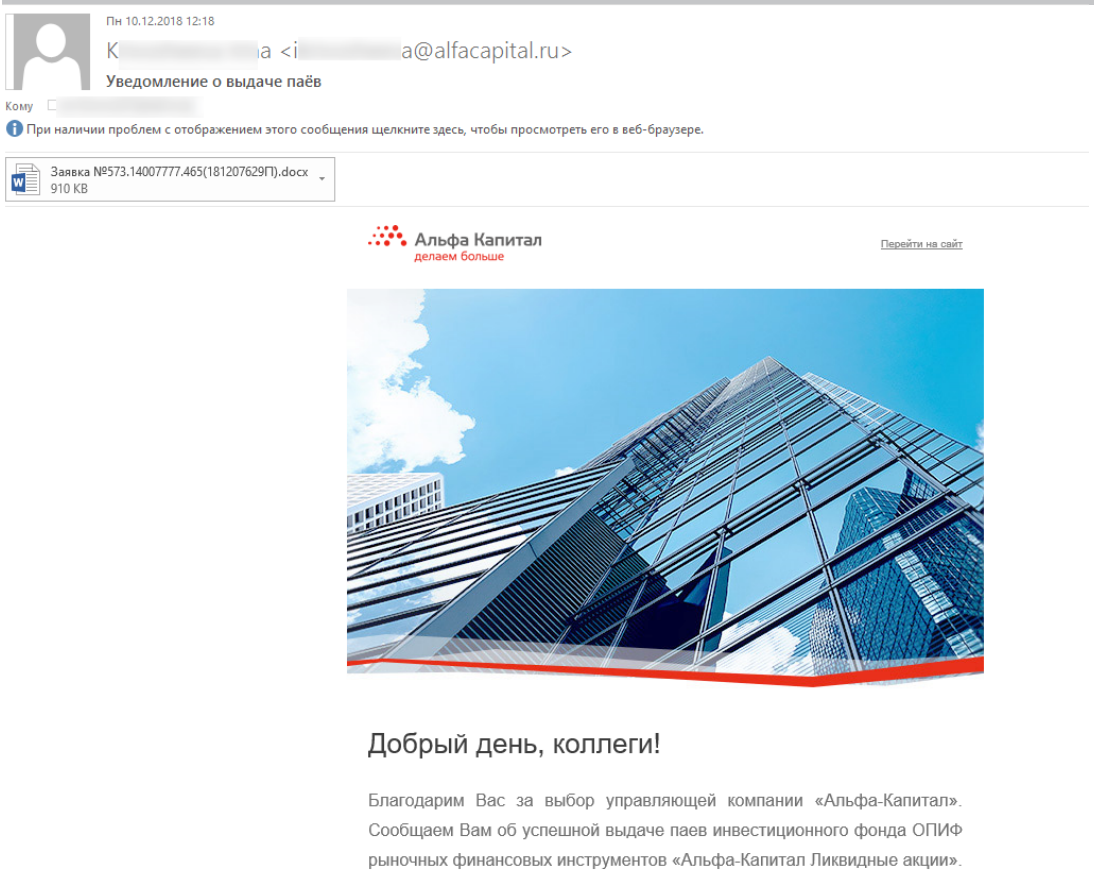
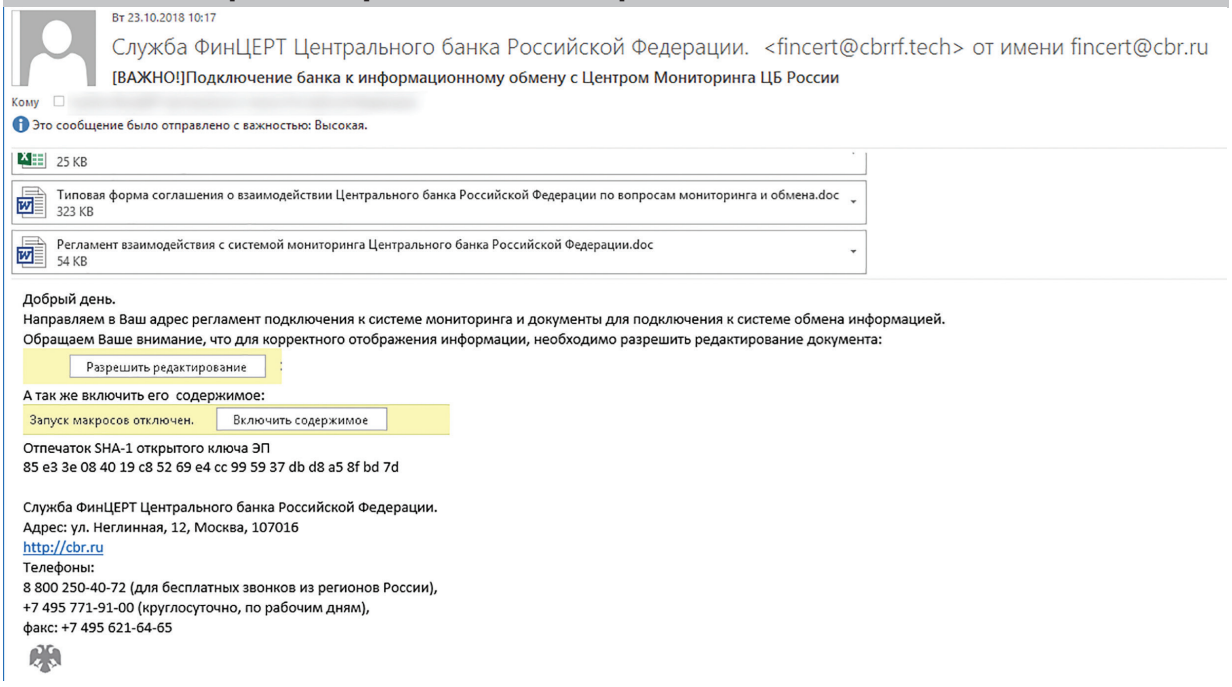


Рис. 8. Пример фишингового письма, рассылаемого новой группировкой, атаковавшей кредитно-финансовый сектор



Резюме: группировки сохраняют активность

Несмотря на общий рост числа атак в 2018 г., финансовый ущерб значительно снизился по сравнению с предыдущим годом. Этому во многом способствует информационный обмен внутри отрасли. Затишье может быть связано и с арестом одного из руководителей группировки Cobalt в марте 2018 г., так как существенная доля успешных хищений в российских банках годом ранее была связана именно с ее деятельностью. Впрочем данная группа продолжает свою деятельность. Не исключено, что после арестов участников Cobalt и FIN7 (Carbanak) преступники формируют новые группировки и проводят реструктуризацию. В конце 2018 г. был выявлен загрузчик группы Silence, подписанный валидным сертификатом SEVA MEDICAL LTD. Этим же сертификатом был подписан один из COM–DLL дропперов группы Cobalt. Это позволяет говорить о возможном смешении составов группировок или об использовании ими одних и тех же сервисов, что весьма вероятно, так как современные киберпреступники все чаще работают по сервисной модели. Злоумышленники разрабатывают новые инструменты, собирают информацию об уязвимостях и совершенствуют техники атак, в том числе улучшают методы доставки полезной нагрузки с помощью фишинга. Это делается и для того, чтобы преодолеть совершенствующиеся средства защиты.

ЗАЩИЩЕННОСТЬ ИНФРАСТРУКТУРЫ КРЕДИТНО-ФИНАНСОВОЙ ОРГАНИЗАЦИИ

Общий тренд: безопасность внутренней сети далека от совершенства

Основные уязвимости и недостатки механизмов защиты сетевого периметра банков подразделяются на четыре типа:

– недостатки конфигурации серверов,
– недостатки управления учетными записями и паролями,
– недостаточная сетевая безопасность,
– уязвимости веб-приложений.

Наиболее часто встречающиеся проблемы в конфигурации серверов – несвоевременное обновление ПО (67% банков) и хранение чувствительных данных в открытом виде (58% банков). Более чем в 50% обследованных банков использовались словарные пароли. В 58% случаев использовались открытые протоколы передачи данных, а в 50% – были доступны интерфейсы удаленного доступа и управления. Среди уязвимостей веб-приложений отметим возможность внедрения SQL-кода (33% банков) и загрузки произвольных файлов (25%), способных привести к выполнению произвольных команд на сервере. При проведении тестов на проникновение в банках в 2017–2018 гг. во всех случаях преодолеть периметр удавалось из-за недостаточной защиты веб-приложений.

Защита сетевого периметра в банковской сфере значительно выше, чем в других отраслях. В ходе тестирования на проникновение (за аналогичный период) сетевой периметр организаций преодолевается в 58%

случаев. В кредитно-финансовой сфере этот показатель составляет 22% и возрастает до 75% при использовании социальной инженерии.

Рис. 9. Доли уязвимых сервисов на сетевом периметре 100 крупнейших банков

Безопасность внутренней сети кредитно-финансовых организаций далека от совершенства. Полный контроль над инфраструктурой был получен во всех банках, исследованных в 2017–2018 годах. В 33% случаев, не обладая максимальными привилегиями в системе, можно получить доступ к узлам, с которых выполняется управление банкоматами, доступ к системам межбанковских переводов, карточному процессингу, платежным шлюзам.

Рис. 10. Наиболее распространенные уязвимости во внутренней сети (доля банков)

Типовые векторы атак во внутренней сети часто базируются на слабой парольной политике и недостаточной защите от восстановления паролей из памяти ОС. Почти в 50% систем слабые пароли устанавливают пользователи, но чаще используются стандартные учетные записи, оставляемые администраторами при установке СУБД, веб-серверов, ОС или создании служебных учетных записей. Приложения часто обладают избыточным привилегиями или содержат известные уязвимости, в итоге злоумышленники имеют возможность получить административные права на узле в 1–2 шага.

Попытки использования банками корпоративных блокчейн-систем создают дополнительные риски. Компоненты этих систем, связь между ними и прочими системами финансовой организации (в том числе внутренними и внешними приложениями) открывают новые возможности для проникновения в инфраструктуру. Оценка безопасности пилотных внедрений технологии блокчейн в банковские проекты показала, что в 71% случаев содержались уязвимости в смарт-контактах, половина проектов имела уязвимости в приложениях, используемых для доступа к данным, хранящимся в блокчейне. Это связано в том числе и с тем, что практика безопасной разработки еще не наработана, а требования по безопасности к внедрению таких систем еще только предстоит сформировать.

Ввиду того, что такая система оперирует критически важными данными, для успешной атаки достаточно лишь одной уязвимости – не важно, в каком компоненте системы. Это сильная мотивация для злоумышленников. В числе последствий атак могут быть несанкционированное внесение данных в реестр, атаки на пользователей со стороны блокчейна, полная блокировка работоспособности системы, проникновение в сеть организации при помощи специально подготовленных блокчейн-транзакций, используемых как транспорт для атак на связанные системы. Гипотетически это может привести к полному контролю со стороны нарушителя над критически важными ресурсами организации.

Ключевые проблемы: неосведомленность персонала и неготовность к оперативному выявлению угроз

Часто самым уязвимым звеном в системе защиты кредитно-финансовой организации является персонал. Оценка осведомленности показала, что в 75% кредитно-финансовых организаций сотрудники переходили по ссылке, указанной в фишинговом письме, в 25% – вводили свои учетные данные в ложную форму аутентификации, и еще в 25% хотя бы один сотрудник запускал на своем рабочем компьютере вредоносное вложение. В среднем в банках по фишинговой ссылке переходили около 8% пользователей, 2% запускали вложенный файл, но свои учетные данные вводили менее 1% пользователей. При этом достаточно, чтобы всего один пользователь выполнил нежелательное действие – и нарушитель получит доступ к корпоративной сети. Таким образом, три четверти банков уязвимы к атакам методами социальной инженерии, использующимися для преодоления периметра почти каждой преступной группировкой.

Другая проблема – низкий уровень защищенности внутренней сети и неготовность к оперативному выявлению угроз. Такие результаты позволяют предположить, что любая преступная группировка смогла бы получить полный контроль над доменной инфраструктурой в каждом из исследованных банков.

Возвращаясь к теме атак на корпоративные блокчейн-системы, следует отметить, что на данный момент затруднены своевременное обнаружение подобных инцидентов (из-за отсутствия общедоступного инструментария) и реагирование на них, так как существует только два варианта реагирования: hard fork блокчейна (то есть откат состояния блокчейна до момента совершения атаки и добавление новых транзакций, начиная с этого момента); и принятие последствий атаки (единственный вариант в случае использования публичного блокчейна). Оба варианта имеют побочные эффекты. При проведении hard fork все транзакции, совершенные после инцидента, будут утеряны, что потребует их добавления заново. Это особенно критично, если данные о случившемся инциденте появились спустя значительное время после атаки.

Резюме: необходимо повысить оперативность выявления атак

Финансовые организации имеют достаточно эффективные барьеры для защиты от внешних атак, но не готовы противостоять нарушителю во внутренней сети. Зная это, злоумышленники обходят системы защиты сетевого периметра с помощью простого и эффективного метода – фишинга, который доставляет вредоносное ПО в корпоративную сеть. Преступники следят за публикацией новых уязвимостей и быстро модифицируют свои инструменты. Внутри сети злоумышленники свободно перемещаются незамеченными с помощью известных уязвимостей и легитимного ПО, не вызывающего подозрений у администраторов. Используя недостатки защиты корпоративной сети, злоумышленники за короткое время получают полный контроль над всей инфраструктурой банка. Сейчас банки должны сосредоточиться на обеспечении безопасности во внутренней сети и внедрении средств защиты, которые позволят оперативно выявлять следы атак в инфраструктуре.

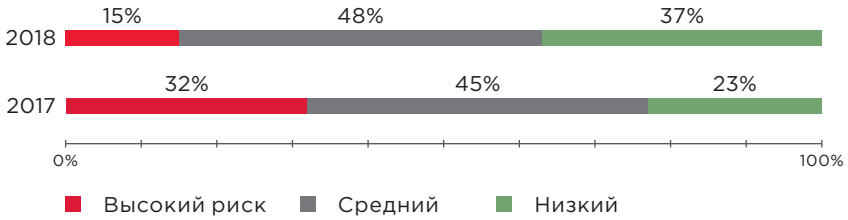
Блокчейн – относительно новая технология, и необходимо особое внимание к построению и эксплуатации основанных на ней систем, в том числе с точки зрения безопасности. Обеспечение безопасности используемых блокчейн-систем требует от кредитно-финансовых организаций внедрения методологии безопасной разработки смарт-контрактов; детального анализа архитектуры и конфигурации инфраструктуры информационной системы, построенной на базе блокчейна; обязательного анализа исходного кода информационной системы и смежных компонентов; регулярной независимой оценки безопасности как самой блокчейн-системы в целом (включая тестирование на проникновение), так и отдельных ее компонентов (смарт-контрактов, веб- и мобильных приложений).

ЗАЩИЩЕННОСТЬ ОНЛАЙН-БАНКИНГА И МОБИЛЬНОГО БАНКИНГА

Общий тренд: пароли, финансовая информация и персональные данные пользователей остаются в зоне риска

К числу ключевых тенденций 2018 г. в области защищенности онлайн-банкинга относится сокращение доли уязвимостей высокого уровня риска (с 32% в 2017 г. до 15% в 2018 г.).

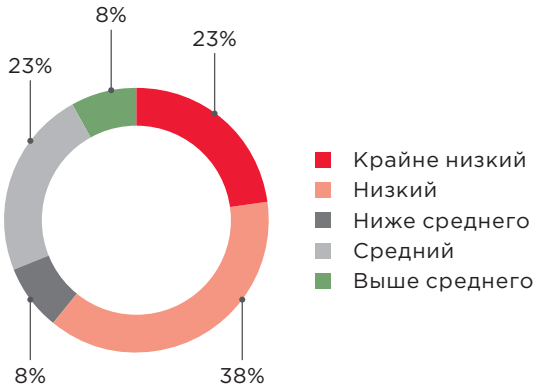
Рис. 11. Доля уязвимостей различного уровня риска



Теряет актуальность критически опасная уязвимость «Недостаточная аутентификация»: в 2018 г. не зафиксировано ни одного приложения, в котором бы она оставалась.

Однако по-прежнему во многих системах операции повышенной важности совершаются без дополнительного (второго) фактора аутентификации. При этом продолжают оставаться под угрозой личная информация клиентов и банковская тайна: риск несанкционированного доступа к личным данным клиентов и банковской тайне (к выпискам по счету или платежным поручениям других пользователей) существует в каждом исследованном в 2018 г. онлайн-банке (по итогам 2017 г. этот показатель составил 94%). Из-за ошибок в логике работы онлайн-банка остается риск мошеннических операций и кражи денежных средств: например, в результате так называемых атак на округление суммы денежных средств при конвертации валюты.

Рис. 12. Уровень защищенности онлайн-банков (доля систем)



В мобильных приложениях уязвимости высокого уровня риска обнаружены в 38% приложений для iOS и 43% приложений для платформ под управлением Android (в 2017 г. уязвимости такого типа обнаружены в 25 и 56% приложений соответственно). Большинство проблем безопасности – общие для обеих платформ. Небезопасное хранение данных – основной недостаток, он выявлен в 76% мобильных приложений (что на 11% выше показателя 2017 г.). Под угрозу попадают пароли, финансовая информация и персональные данные пользователей. Злоумышленнику редко требуется физический доступ к смартфону, чтобы украсть данные: 89% уязвимостей могут быть использованы с использованием ВПО.

Ключевые проблемы: ошибки бизнес-логики систем и уязвимости кода

Онлайн-банки

На первое место вышли ошибки в реализации механизмов двухфакторной аутентификации: в некоторых онлайн-банках не применяются одноразовые пароли (one-time password, OTP) для критически важных действий (аутентификация, смена учетных данных и другое) или пароли имеют слишком большой срок действия. Это может быть связано с тем, что банки стремятся найти баланс между безопасностью и удобством использования приложений. Так, ради удобства применения и возможности сэкономить на СМС-сообщениях для OTP в системах ДБО сегодня часто используют механизмы адаптивной аутентификации, в частности риск-ориентированную модель аутентификации (risk-based authentication). Однако отказ даже от части мер безопасности в пользу удобства повышает риск совершения мошеннических операций. Так, если нет необходимости подтверждать операцию с помощью одноразового пароля, злоумышленнику больше не требуется доступ к мобильному телефону жертвы, а слишком большой срок действия пароля повышает шанс его успешного подбора.

В 2018 г. до 31% выросла (в 2017 г. – 6%) доля приложений, в результате атак на которые злоумышленник может повлиять на бизнес-логику системы (в 2017 г. – 6%). Вероятно, это связано с ростом числа уязвимостей в коде приложений, разработанных банками самостоятельно. В 2018 г. доля таких уязвимостей достигла 59%, в то время как в 2017 г. она составляла 39%. Системы ДБО, разработанные банками самостоятельно, являются более уязвимыми по сравнению с готовыми решениями: среднее число уязвимостей в приложениях собственной разработки в три раза больше, чем в системах, предлагаемых вендорами (в 2017 г. оба показателя были близки по своему значению).

Большинство уязвимостей и у вендоров, и в собственных разработках относится к уязвимостям кода. Но вендоры чаще допускают ошибки на этапе проектирования, а в собственных решениях банков уязвимости закладываются на этапе написания кода. К этой группе относятся, например, «Межсайтовое выполнение сценариев» и «Внедрение SQL-кода».

Разработчики систем ДБО сосредоточены на функциональных возможностях больше, чем на безопасности. Как следствие, 75% уязвимостей в покупных решениях связаны с недостатками механизмов защиты. Примеры уязвимостей в механизмах защиты – «Недостаточная защита от подбора учетных данных», «Недостаточная авторизация».

К числу наиболее распространенных уязвимостей конфигурации относится раскрытие чувствительных данных в сообщениях об ошибках и версиях используемого ПО в заголовках ответов веб-сервера.

Мобильный банкинг

Общий уровень защищенности клиентских частей мобильных приложений для Android и iOS примерно одинаков. Около трети всех уязвимостей в клиентских частях мобильных приложений для обеих платформ имеет высокий уровень риска. Аутентификационные данные небезопасно хранятся в 53% мобильных приложений.

Серверные части мобильных приложений в равной степени содержат уязвимости в коде самого приложения и в механизмах его защиты. В числе последних стоит отметить недостатки реализации двухфакторной аутентификации, позволяющие злоумышленнику совершать операции от имени законного пользователя, например переводить деньги с его счета на свой.

В среднем каждая серверная часть содержит пять уязвимостей кода и одну уязвимость конфигурации. Недостаточная авторизация выявлена в 43% серверных частей в 2018 г. (в 2017 г. – в 50%). Это один из самых распространенных недостатков высокого уровня риска, его доля составила 45% от всех критически опасных уязвимостей.

Большинство недостатков связано с ошибками в механизмах защиты: 74% (в 2017 г. – 75%) и 57% (66%) – для приложений на iOS и Android соответственно, 42% (75%) – для серверных частей. Такие уязвимости возникают на этапе проектирования, а их устранение требует внесения существенных изменений в код.

Резюме: общий уровень защищенности приложений для банкинга остается недостаточным

Несмотря на сокращение доли уязвимостей высокого уровня риска, защищенность онлайн-банков остается низкой. Одно из серьезнейших последствий атаки на них – кража денежных средств. В 2018 г. эта угроза отмечалась в 54% онлайн-банков (в 2017 г. этот показатель был на 4% ниже). Угроза несанкционированного доступа к информации клиентов и банковской тайне актуальна для каждого исследованного онлайн-банка, а в отдельных случаях уязвимости позволяли развивать атаку до проникновения в корпоративную инфраструктуру.

При разработке мобильных приложений безопасности уделяется недостаточно внимания, и основная проблема связана с небезопасным хранением данных; злоумышленники могут получить данные банковских карт и персональные данные пользователей.

Мобильные и онлайн-банки – популярные каналы для атаки на клиентов финансовых организаций. Общее повышение уровня защищенности финансовых организаций, а также то, что атаки на онлайн-банки не требуют такой высокой квалификации и подготовки, как атаки на инфраструктуру, может привести к переключению внимания части злоумышленников с финансовых организаций на их клиентов. В первую очередь под угрозой юридические лица, поскольку у них можно украсть более крупные суммы денег.

ЗАЩИЩЕННОСТЬ БАНКОМАТОВ, ПЛАТЕЖНЫХ ТЕРМИНАЛОВ

Общий тренд: blackbox продолжают лидировать

Логические атаки на банкоматы набирают популярность с 2009 г., когда был обнаружен троян Skimer, позволяющий похищать деньги и данные платежных карт. Skimer продолжает развиваться и по сей день, а наряду с ним появляются все новые семейства вредоносных программ – GreenDispenser, Alice, Ripper, Radpin, Ploutus и другие, продающиеся на форумах дарквеба. Цены на них начинаются от 1500 долл. США, но потенциальная прибыль значительно превышает расходы. В 2017 г. было обнаружено ПО CutletMaker, свободно продававшееся вместе с подробной инструкцией по использованию за 5000 долл. США.

В начале 2018 г. в США прошла волна «джекпоттинга»: преступники устанавливали на банкоматы вредоносное ПО Ploutus-D, позволявшее управлять выдачей наличных. В арсенале преступников присутствовал медицинский эндоскоп – с его помощью они проходили физическую аутентификацию без доступа к сейфу.

Хотя доля атак на банкоматы и POS-терминалы за год сократилась с 3 до 1% от общего числа инцидентов, они по-прежнему остаются в тренде. По данным Европейской ассоциации безопасных транзакций (The European Association for Secure Transactions, EAST), в 2018 г. было зафиксировано 157 логических атак на банкоматы, причем 156 из них относились к типу blackbox.

Ключевые проблемы: blackbox и доступ к банкомату изнутри локальной сети

Все уязвимости, встречающиеся при анализе защищенности банкоматов, делятся на четыре группы:

1. Недостатки сетевой безопасности, позволяющие злоумышленнику, который получил доступ к сети банкомата, проводить атаки на сетевое оборудование, на доступные сетевые службы, перехватывать и подменять трафик. Такие атаки могут позволить подменить ответы процессингового центра или получить контроль над банкоматом. В исследуемых системах часто выявлялись недостатки межсетевого экранирования (88% банкоматов) и недостаточная защита данных, передаваемых между банкоматом и процессинговым центром (шифрование передаваемых данных отсутствовало в 58% банкоматов).

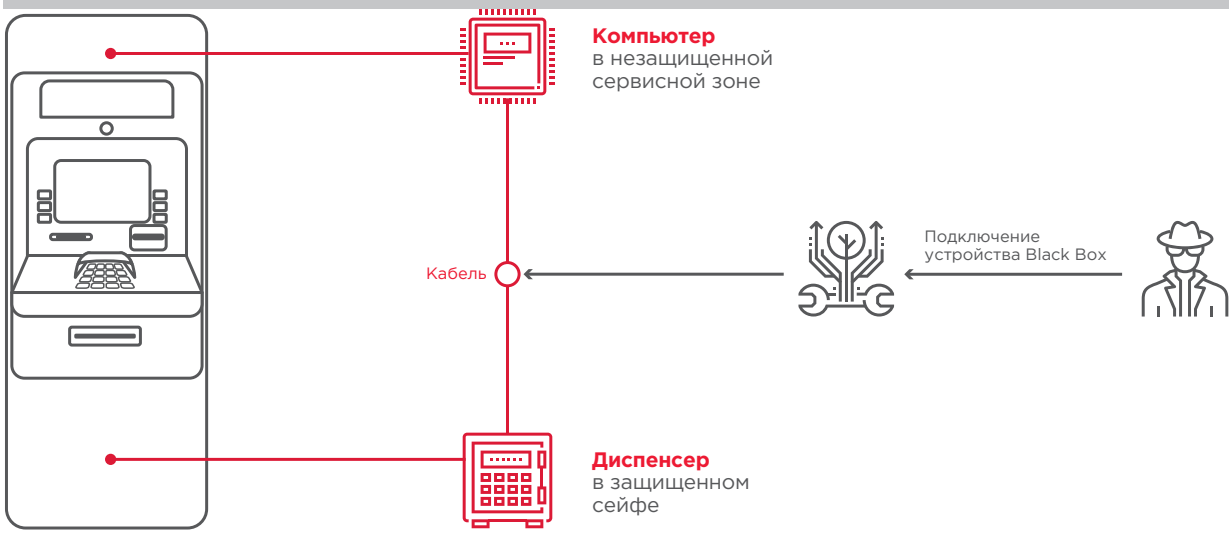
2. Недостатки защиты периферийных устройств, например отсутствие аутентификации между периферийным оборудованием и ОС банкомата (96% банкоматов), позволяют преступнику обращаться к этим устройствам после заражения банкомата вредоносным ПО или напрямую подключать свое оборудование к диспенсеру или картридеру. Это может привести к краже денег или перехвату данных платежных карт.

3. Недостатки конфигурации систем и устройств, то есть пробелы в защите, которыми злоумышленник может воспользоваться, имея доступ в сервисную зону, – например, отсутствие шифрования жесткого диска (92% банкоматов), недостаточная защита от выхода из режима «киоска» (85%), возможность подключения произвольных устройств (81%).

4. Уязвимости и недостатки конфигурации приложений класса Application Control: они направлены на предотвращение выполнения постороннего кода в системе, однако на поверку оказались недостаточно эффективными в 88% случаев. Уязвимости могут изначально содержаться в их коде или появиться как результат неправильной конфигурации.

Основные типы атак, которые были зафиксированы в России в 2018 г., – это blackbox и доступ к банкомату изнутри локальной сети банка. Атака blackbox подразумевает возможность напрямую подключить к диспенсеру свое устройство, запрограммированное на отправку команд для выдачи купюр.

Рис. 13. Атака blackbox

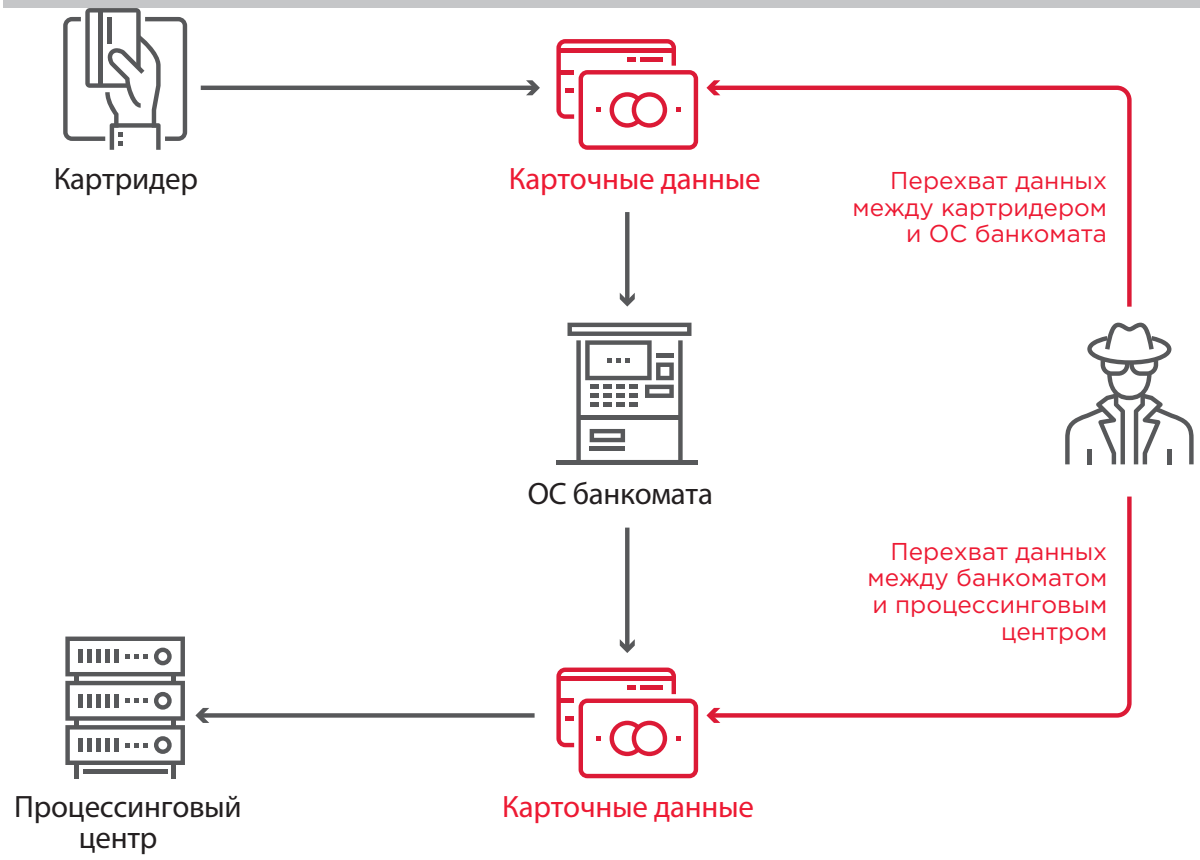


Результаты работ по анализу защищенности банкоматов, проведенных в 2017–2018 гг., показывают, что к такой атаке уязвимы 69% банкоматов. Причина этого в 50% случаев – использование недостаточно надежного шифрования между диспенсером и ОС, а еще в 19% – отсутствие каких-либо мер защиты против blackbox. На некоторых моделях банкоматов для проведения атаки преступнику требуется всего 10 минут.

При проведении тестов на проникновение доступ к управлению банкоматами из внутренней сети удалось получить в 25% банков. Это связано с общим низким уровнем защищенности во внутренней сети банков.

Во всех исследуемых банкоматах был возможен перехват данных с магнитной полосы карты из-за отсутствия аутентификации и шифрования данных при взаимодействии с картридером, а в 58% банкоматов – из-за отсутствия шифрования при передаче данных между банкоматом и процессингом.

Рис. 14. Варианты атак, направленных на перехват карточных данных



Резюме: велик риск новых атак со стороны кибергруппировок и неквалифицированных злоумышленников

Уязвимости, связанные с сетевой безопасностью, недостатками конфигурации, недостаточной защитой периферийных устройств, в совокупности позволяют похитить деньги из банкомата или перехватить данные банковских карт. Используемые механизмы безопасности не являются серьезным препятствием для атаки: почти во всех случаях была выявлена возможность обхода установленных средств защиты. Часто одна и та же конфигурация используется на множестве банкоматов, поэтому успешная атака на один банкомат позволяет преступникам провести серию аналогичных с использованием одного сценария. На теневом рынке спрос на ВПО для банкоматов остается высоким, а значит, следует готовиться к новым атакам как со стороны крупных преступных группировок, так и низкоквалифицированных хакеров.

ЗАЩИЩЕННОСТЬ ПЛАТЕЖНЫХ ТЕРМИНАЛОВ (POS)

Общий тренд: mPOS`ы защищены недостаточно

В последние годы число операций, выполняемых с помощью mPOS-терминалов, существенно возросло. Острая конкуренция среди поставщиков mPOS привела к упрощению получения платежного терминала. Как и обычные POS-терминалы, они являются конечным звеном платежной инфраструктуры. Это делает их интересными и легко доступными для злоумышленников. Больше 50% исследованных mPOS-терминалов уязвимы для атак, при этом в целом уязвимыми оказались все проанализированные поставщики mPOS-терминалов. Зарегистрированы многочисленные серьезные проблемы безопасности, в частности уязвимость для выполнения произвольных команд, подделки суммы и выполнения удаленного кода. Аппаратные механизмы защиты терминалов в большинстве случаев надежны и развиты. Однако другие аспекты защищены гораздо слабее.

Ключевые проблемы: от выполнения произвольных операций до перехвата данных

Злоумышленник может подключиться к устройству через bluetooth и осуществлять произвольные операции. Для этого ему нужна информация о bluetooth-сервисах, запущенных на устройстве, а также соответствующих характеристиках и функциях. Эту информацию можно получить с помощью реверс-инжиниринга до проведения атаки. Злоумышленнику потребуется лишь доступ к mPOS-терминалу, телефон, который поддерживает регистрацию событий интерфейса хост-контроллера (HCI), и мобильное приложение. Этот вектор атаки может использоваться совместно с эксплуатацией других уязвимостей, чтобы предложить клиенту менее безопасные типы операций, например по магнитной полосе.

Исследования показали наличие риска перехвата HTTPS-трафика между мобильным приложением и сервером платежной системы с последующим изменением суммы транзакции. Недобросовестный продавец может обманным путем заставить владельца карты подтвердить операцию на гораздо большую сумму.

Часть протестированных терминалов уязвима для удаленного выполнения кода, что может обеспечить злоумышленнику полный доступ к ОС терминала. После получения полного доступа к операционной системе злоумышленник сможет перехватить данные Track2 до шифрования или включить незашифрованный режим (для отправки команды) на клавиатуре терминала для перехвата PIN-кода.

Резюме: упрощение входа на рынок карточных платежей не снимает ответственности за их безопасность

Разработчики mPOS-терминалов подчеркивают простоту регистрации и использования устройств. Это ключевые элементы бизнес-модели, но она не учитывает, что снижение барьеров входа на рынок карточных платежей должно сопровождаться существенным увеличением безопасности. Нет сомнений в том, что мошеннические действия продавцов оста-

нутся серьезной проблемой поставщиков mPOS-терминалов. Необходимо разработать серьезный подход к проблеме безопасности, включая проверку в ходе регистрации и строгий мониторинг платежей.

ЗАЩИЩЕННОСТЬ ИНВЕСТИЦИОННЫХ И ТРЕЙДИНГОВЫХ ПРИЛОЖЕНИЙ

Общий тренд: существенный риск проведения несанкционированных операций

Выбирая торговую платформу, трейдеры руководствуются функциональностью, облегчающей их задачи. Однако не все задумываются о безопасности этих приложений. Если хакер получит доступ к какой-то из функций – скажем, сможет изменить параметры автоматического закрытия сделки, – трейдер потерпит убытки. Кроме того, в личных кабинетах пользователей хранится конфиденциальная информация: данные о сделках, история операций, информация о доступных средствах на балансе. Исследования показали, что популярные торговые терминалы не защищены от атак: уязвимости найдены в каждом исследованном приложении, при этом 72% приложений содержали хотя бы одну критически опасную уязвимость. Во всех случаях недостатки защиты позволяли атаковать пользователей.

Рис. 15. Угрозы, представляющие наибольшую опасность для трейдеров

33% изученных приложений имели уязвимости, позволяющие проводить финансовые операции от имени других пользователей. Такие атаки могут вызвать изменение цен на рынке, отразиться на большом количестве пользователей, затронуть частных трейдеров и крупные компании – банки, международные торговые корпорации, финансово-инвестиционные организации; вызвать беспорядки на бирже и привести к потере денег.

Ключевые проблемы: недостатки шифрования, небезопасное хранение данных, риск перехвата данных

Мы выделяем два вероятных сценария атак:

1. Трейдер с одного и того же устройства пользуется торговым терминалом и посещает сайты в Интернете. На одном из посещаемых им сайтов хакер разместил вредоносный JavaScript-код, который, не требуя дополнительных действий со стороны пользователя, атакует его терминал и покупает или продает активы. Антивирус не отреагирует на выпол-

нение вредоносного кода, поскольку для атаки не нужно загружать файл на компьютер пользователя или выполнять команды в ОС.

2. Злоумышленник находится в одной сети с трейдером (например, трейдер подключен к сети по wi-fi или через оборудование, которое контролирует злоумышленник). Так злоумышленник сможет перехватывать и изменять трафик пользователя. Атака возможна и в том случае, если канал связи недостаточно защищен и перехват трафика происходит на стороне провайдера.

Уязвимости, обнаруженные в десктопных приложениях, преимущественно заключались в отсутствии шифрования передаваемых данных (42%) и возможности выполнения произвольных команд (29%). Атаки на десктопные приложения могут привести к тому, что злоумышленник получит контроль над компьютером трейдера и сможет развивать атаку на инфраструктуру организации.

В мобильных приложениях большинство уязвимостей (57%) было связано с небезопасным хранением данных. При анализе веб-приложений были обнаружены уязвимости в коде и конфигурации, во всех приложениях отсутствовали HTTP-заголовки, обеспечивающие дополнительную защиту от некоторых видов атак (например, от атак типа Clickjacking и «Межсайтовое выполнение сценариев»). Атаки на веб-приложения могут носить массовый характер и оказывать существенное влияние на изменение цен.

Резюме: атаки на пользователей трейдинговых систем могут стать реальностью

Сегодня атаки на приложения для трейдинга еще не распространены, злоумышленники, возможно, только изучают потенциальные способы атак. Однако в силу слабой защищенности трейдинговых приложений и традиционного стремления злоумышленников к легкой масштабируемости и быстрой монетизации атаки на пользователей трейдинговых систем имеют все шансы превратиться в массовые в ближайшее время.

ОБЩИЕ ВЫВОДЫ, ПРОГНОЗЫ И РЕКОМЕНДАЦИИ POSITIVE TECHNOLOGIES

В 2018 г. на фоне увеличения общего количества кибератак на кредитно-финансовые организации наблюдалось значительное снижение финансового ущерба. Уменьшение числа успешных атак во многом связано с деятельностью ФинЦЕРТ, но еще один немаловажный фактор – это арест участников крупных преступных группировок. В ближайшее время возможно появление ряда новых группировок и инструментов, что спровоцирует новую волну атак.

Защита сетевого периметра финансовых организаций находится на достаточно высоком уровне, поэтому основным методом проникновения в инфраструктуру финансовых организаций останется доставка вредоносного ПО путем фишинговых рассылок. Стоит ожидать, что преступники будут вкладывать значительные средства в закупку неопубликованных эксплойтов для уязвимостей нулевого дня на теневом рынке.

Общее повышение уровня защищенности финансовых организаций может привести к тому, что часть злоумышленников попробует свои силы на других целях: клиентах банков, платежных устройствах и банкоматах. Проблемы, выявляемые при анализе защищенности банкоматов, платежных терминалов и финансовых приложений, говорят об острой необходимости совершенствования систем защиты.

Мы рекомендуем финансовым организациям активно участвовать в обмене информацией о кибератаках и индикаторах компрометации. Центры мониторинга и реагирования на инциденты (например, ФинЦЕРТ Банка России) помогают значительно снизить успешность кибератак на кредитно-финансовую сферу. Кроме того, необходимо быть готовым оперативно выявлять следы атак в своей инфраструктуре. Крайне важно постоянно отслеживать аномальную активность в сети своей компании, чтобы обнаруживать и исследовать новые неизвестные атаки, делиться такой информацией с другими финансовыми организациями.

Обнаружить атаку хорошо подготовленной кибергруппировки в момент проникновения в локальную сеть сегодня невозможно, крайне сложно сделать это и на этапе закрепления и распространения в инфраструктуре. Зачастую ситуация усугубляется неготовностью самой инфраструктуры атакованной организации к выявлению атак. Надеяться на защиту отдельных серверов и рабочих станций с помощью типовых решений бесполезно. Сегодня важно понимать, насколько эффективны те системы, которые внедрены в компании для обеспечения безопасности ключевых активов. Преступники уже давно научились обходить антивирусы, «песочницы», системы обнаружения вторжений. Компаниям необходимо реализовать комплексный подход, позволяющий сузить круг возможностей нарушителя и обеспечить максимальное понимание происходящих в инфраструктуре событий безопасности в контексте системных журналов, трафика и объектов, циркулирующих в сети. Только в этих условиях возможно построение процесса Threat Hunting, позволяющего успешно выявлять действия группировок уже внутри инфраструктуры.

Глубокий анализа трафика, ретроспективный анализ событий ИБ, профилирование действий пользователей и возможность исследования оперативной памяти, процессов и других форензик-артефактов позволяют значительно сократить время присутствия злоумышленников в инфраструктуре и предотвратить достижение поставленных ими целей. И, конечно, средства защиты будут неэффективны без поддержки высококвалифицированных специалистов в области расследования инцидентов.

ПРИЛОЖЕНИЕ 3

SOLAR JSOC – КИБЕРАТАКИ НА ФИНАНСОВО-КРЕДИТНЫЕ ОРГАНИЗАЦИИ В 2018 ГОДУ

Отчет Solar JSOC Security Flash Report основан на данных за 2018 г., полученных в центре мониторинга и реагирования Solar JSOC. В документе отражена сводная информация о выявленных инцидентах по различным категориям. Отчет демонстрирует, кто, как, в какое время и с использованием каких векторов и каналов атаковал российские компании.

Solar JSOC Security Flash Report предназначен для информирования служб ИТ и информационной безопасности о текущем ландшафте угроз и основных трендах кибератак.

МЕТОДОЛОГИЯ

Solar JSOC Security Flash Report базируется на анализе инцидентов, выявленных командой Solar JSOC как в рамках оказания своих регулярных услуг мониторинга и реагирования на кибератаки, так и на уровне консультативно-аналитической поддержки компаний российского рынка.

Одним из ключевых факторов, влияющих на методологию исследования, является проактивность сервисов Solar JSOC, которые позволяют выявлять действия злоумышленников на самых ранних стадиях и до проникновения в инфраструктуру. Это накладывает определенные ограничения на проведение оценки финансового ущерба организации (в силу отсутствия фактических потерь), а также идентификацию целей злоумышленника: направлены ли его действия на получение финансовой выгоды, сбор чувствительной информации, закрепление в инфраструктуре с целью дальнейшей продажи ресурсов, хактивизм или иное. Поэтому при определении целей злоумышленника Solar JSOC использует комбинированную методику, которая опирается на следующие особенности атаки:

- При выявлении инцидентов на ранней стадии (до фактического закрепления злоумышленников и развития атаки в инфраструктуре) учитываются используемые техники и методики атаки, функционал используемого вредоносного ПО и его применимость для достижения конкретных целей, атрибуция хакерской группировки и информация о ее типовых целях, информация о схожих атаках (получаемая в рамках информационных обменов или коммерческих расследований инцидентов) с известным ущербом и целями злоумышленников.
- При выявлении атаки на фазе распространения (в рамках инцидентов, детектируемых у новых подключаемых заказчиков до момента стабилизации уровня безопасности инфраструктуры) на фактическом перечне скомпрометированных хостов дополнительно учитывается: их территориальная распределенность, функцио-

нальное назначение, возможности реализации одной из вышеприведенных целей, а также динамика и вектор движения киберпреступника. Например, если первые действия злоумышленника после попадания в инфраструктуру направлены на проникновение на хосты, связанные с финансовыми операциями и выводом денежных средств, то такая атака классифицируется как нацеленная на вывод денежных средств. В случае же если при проведении атаки не задействованы специализированные модули для вывода средств, а ее развитие подразумевает широковещательное получение контроля над различными активами инфраструктуры, то атака классифицируется как нацеленная на захват инфраструктуры.

- При выявлении атак на финальной стадии (в рамках расследований инцидентов у новых клиентов, не использующих сервисы мониторинга на момент инцидента) дополнительно собирается информация о фактическом ущербе, которая в дальнейшем служит ключевым критерием, определяющим вектор атаки.

СВОДНАЯ СТАТИСТИКА ЗА ОТЧЕТНЫЙ ПЕРИОД

- Совокупно в рамках предоставления сервиса заказчикам финансового сектора Solar JSOC обеспечивает контроль и выявление инцидентов для:
  - более 300 внешних сервисов, представленных в сети Интернет;
  - более 9000 серверов общего, инфраструктурного и прикладного назначения;
  - более 60 тыс. сотрудников финансово-кредитных организаций.
- Средний суточный поток событий ИБ, обрабатываемых SIEM-системами и используемых Solar JSOC для предоставления сервиса, составил **9,6 млрд событий**.
- Всего за 2018 г. Solar JSOC зафиксировал в кредитно-финансовых организациях **120 165 событий с подозрением на инцидент**.
- **Доля критичных инцидентов в 2018 г. составила 13%.** Процент существенно ниже среднего по рынку, поскольку в кредитно-финансовых организациях достаточно высокий уровень как общей защищенности инфраструктуры, так и оснащенности современными средствами и технологиями защиты. Это позволяет выявлять атаки злоумышленников на ранних стадиях, до того, как инцидент приобретет статус критичного.
- Среднее время принятия инцидента в работу специалистом Solar JSOC составило 17 минут с момента выявления. Среднее время на подготовку и предоставление аналитической справки об инциденте и рекомендаций с момента возникновения инцидента – 26 минут по критичным инцидентам и 72 минуты – по всем остальным.
- Соблюдение клиентских SLA за 2018 г. составило **98,7%**.

- **60,4%** исследованных событий были зафиксированы при помощи основных сервисов ИТ-инфраструктуры и средств обеспечения базовой безопасности: межсетевые экраны и сетевое оборудование, VPN-шлюзы, контроллеры доменов, почтовые серверы, базовые средства защиты (антивирусы, прокси-серверы, системы обнаружения вторжений). Это свидетельствует о том, что полноценная эксплуатация и качественная настройка даже базовых средств защиты способны серьезно повысить уровень информационной безопасности организации. Во многом это возможно благодаря развитию системы информационных обменов и CERT, передающих широкому перечню контрагентов информацию о новых способах атак, видах вредоносного ПО и уязвимостях.
- Оставшиеся инциденты (**39,6%**) выявляются при помощи сложных интеллектуальных средств защиты или анализа событий бизнес-систем. Они позволяют увидеть более полную картину защищенности компании и своевременно предотвратить критичные таргетированные атаки.

Ключевые тенденции 2018 года

- Во второй половине 2018 г. на **50%** выросло количество атак, направленных на получение контроля над инфраструктурой, на **60%** – количество атак, нацеленных на кражу денежных средств. Мы прогнозируем дальнейший рост атак этих категорий, в случае попыток вывода денежных средств – вплоть до двукратного.
- Киберпреступники наращивают как сложность инструментария, так и темпы его создания. Группировка Cobalt начала рассылку вредоносного ПО, эксплуатировавшего уязвимость CVE-2018-15982, менее чем через двое суток с момента публикации информации о ней. По нашим прогнозам, такое время time-to-virus постепенно станет нормой для всех хакерских группировок. Это потребует от банковских ИТ- и ИБ-подразделений более серьезной, системной и постоянной работы по оперативному тестированию и установке обновлений информационных систем или поиску компенсирующих мер для выявления и противодействия новым векторам атаки.
- На каждом проекте по анализу уровня защищенности в банковских приложениях обнаруживается **как минимум четыре логические уязвимости**, в том числе позволяющие осуществлять атаки класса IDOR. В результате такой атаки злоумышленник может узнать номер счета клиента и остаток средств на нем, а также перевести деньги на сторонний счет, минуя OTP. Уязвимости класса XSS также обнаруживаются в **каждом** банковском приложении.
- **68%** сложных целенаправленных атак начинаются с фишинга. В среднем каждый шестой пользователь, не прошедший курсы повышения осведомленности, поддается на методы социальной инженерии. Однако этот показатель может варьироваться в за-

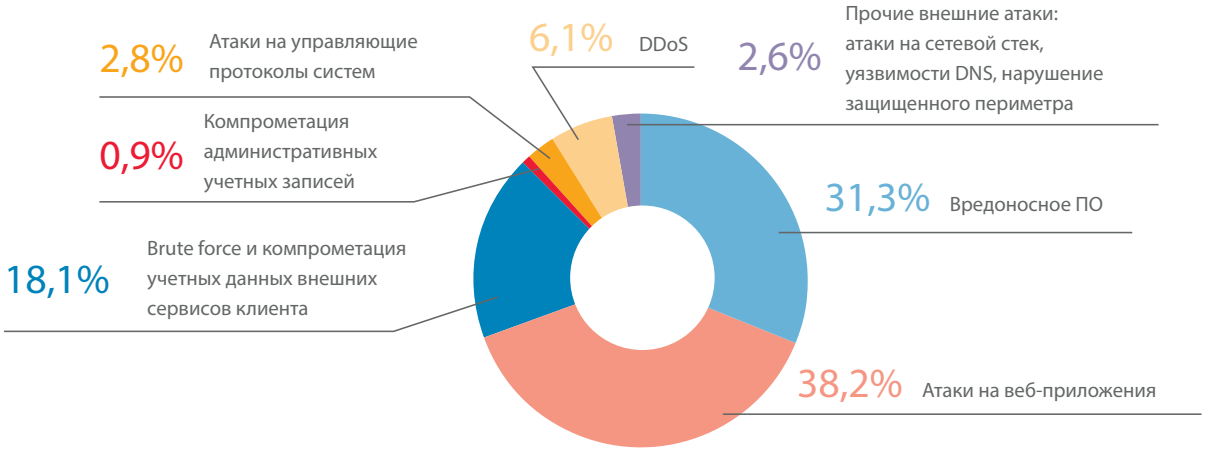
висимости от функционального подразделения компании. В юридической службе жертвой фишинга становится в среднем каждый третий сотрудник, в бухгалтерии, финансово-экономической службе – каждый четвертый, в секретариате и службе техподдержки – каждый шестой.

- В **26%** случаев первым объектом сложной целенаправленной атаки становятся веб-приложения, в том числе интернет-банк.
- По сравнению с 2017 г. количество DDoS-атак выросло более чем в два раза – на **133%**. На наш взгляд, во многом это связано с их дешевизной и эффективностью, которая будет способствовать увеличению числа атак и в 2019 году.
- Большая доля инцидентов ИБ в банках связана с компрометацией учетных записей. Рядовые пользователи зачастую продолжают использовать устаревшие и небезопасные механизмы доступа к рабочим станциям или целевым системам. Учитывая, что пароли сотрудников в корпоративных системах и внешних публичных сервисах часто совпадают, сохраняются риски компрометации инфраструктуры через учетные данные непривилегированного пользователя. Эти риски возрастают, если мы имеем дело с менеджерами среднего и высшего звена. Нередко им позволяют понижать уровень стойкости паролей и/или частоту его смены, что делает такие учетные записи уязвимыми для атаки простым перебором (брутфорс).

ВНЕШНИЕ КИБЕРАТАКИ НА ФИНАНСОВЫЙ СЕКТОР

В этой части отчета рассматриваются инциденты, причиной которых становились действия лиц, не являющихся внутренними пользователями организаций. Из отчета исключены так называемые простые атаки, не ведущие к реальным инцидентам информационной безопасности, – в частности, деятельность автоматизированных систем (бот-сетей), сканирование сетей, неуспешная эксплуатация уязвимостей и подборы паролей.

Рис. 1. Направления атак, 2018 год



Ключевые тенденции и цифры

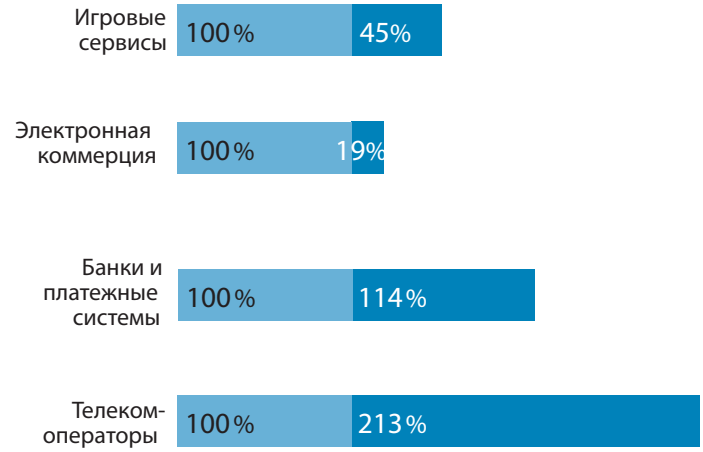
- Серьезно растет количество инцидентов, связанных с заражениями вредоносным ПО. Это свидетельствует не столько об увеличении числа различных вредоносных программ, сколько о ширине охвата и массовости вредоносных рассылок. Все чаще письма, ориентированные на банковский сектор, выявляют в энергетических компаниях, органах государственной власти и промышленных предприятиях. Нерелевантный таргетинг не делает рассылки менее опасными, поскольку часть сотрудников все равно открывает вредоносные письма, а злоумышленник после получения доступа к инфраструктуре может развивать атаку по своему усмотрению, в том числе догружать дополнительные функциональные модули ВПО, ориентированные уже непосредственно на организации именно этой конкретной отрасли.
- По-прежнему часто фиксируются новые экземпляры вредоносного ПО (шифровальщики, криптомайнеры), использующие уязвимость CVE-2017-0144 (EternalBlue), несмотря на то, что с момента появления массовых вирусных эпидемий прошло уже два года. По всей видимости, ряд российских компаний все еще уязвимы к этой атаке.
- В банках доля инцидентов, связанных с компрометацией административных учетных записей, существенно ниже, чем в организациях других сфер деятельности. Такая ситуация обусловлена зрелым подходом к обеспечению безопасности работы привилегированных пользователей в банках. В частности, широкое распространение получили двухфакторная аутентификация для подключений в рамках удаленного доступа, а также подсистемы управляемого терминального доступа или контроля действий администратора, которые затрудняют злоумышленнику проникновение в инфраструктуру даже в случае компрометации пароля.
- По-прежнему высок процент инцидентов, связанных с компрометацией непривилегированных учетных записей. Рядовые пользователи зачастую продолжают использовать устаревшие и небезопасные механизмы доступа к рабочим станциям или целевым системам. Учитывая, что пароли сотрудников в корпоративных системах и внешних публичных сервисах часто совпадают, сохраняются риски компрометации инфраструктуры через учетные данные непривилегированного пользователя. Эти риски возрастают, если мы имеем дело с менеджерами среднего и высшего звена. Нередко им позволяют понижать уровень стойкости паролей и/или частоту его смены, что делает такие учетные записи уязвимыми для атаки простым перебором (брутфорс).

DDoS-атаки

В банковском сегменте DDoS-атаки обычно направлены на мобильный или интернет-банк. Этот вектор может быть использован как злоумышленниками (например, в целях вымогательства в обмен на прекращение атаки), так и конкурентами (в целях нанесения репутационного ущерба, как часть информационной атаки и так далее).

По сравнению с 2017 г. количество DDoS-атак на банки выросло более чем в два раза – на 133%. На наш взгляд, во многом это связано с их дешевизной и эффективностью, которые будут способствовать увеличению числа атак и в 2019 году. При этом рост среднего числа атак на одного клиента финансового сектора составил 114%.

Рис. 2. Рост числа атак на одного клиента (сравнение с другими отраслями)



Самая продолжительная атака, зафиксированная «Ростелекомом» в 2018 г., длилась 820 часов (более 34 суток).

Рис. 3. Самые интенсивные DDoS-атаки (Гбит/с), 2018 год

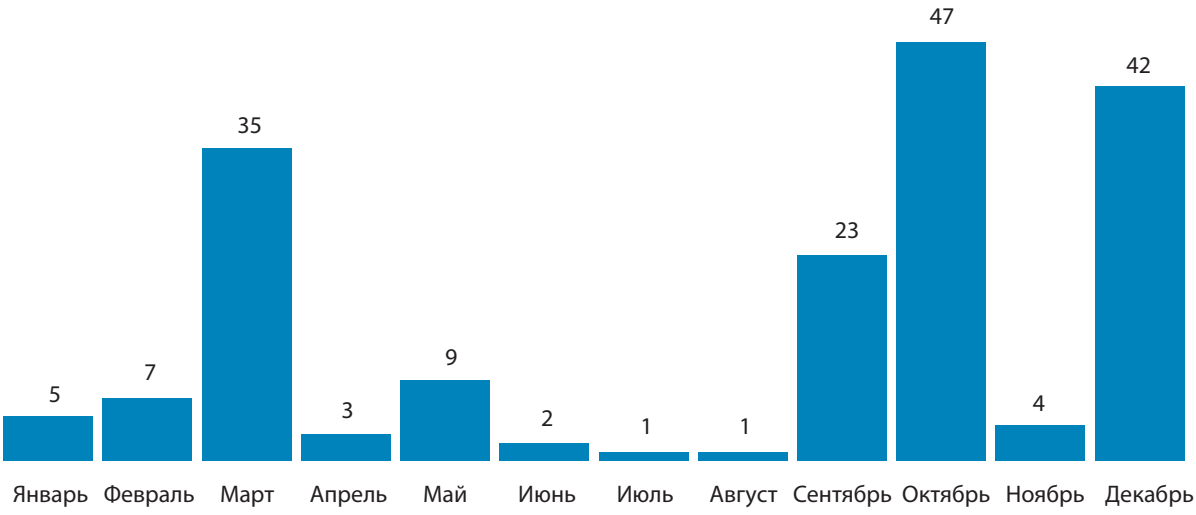
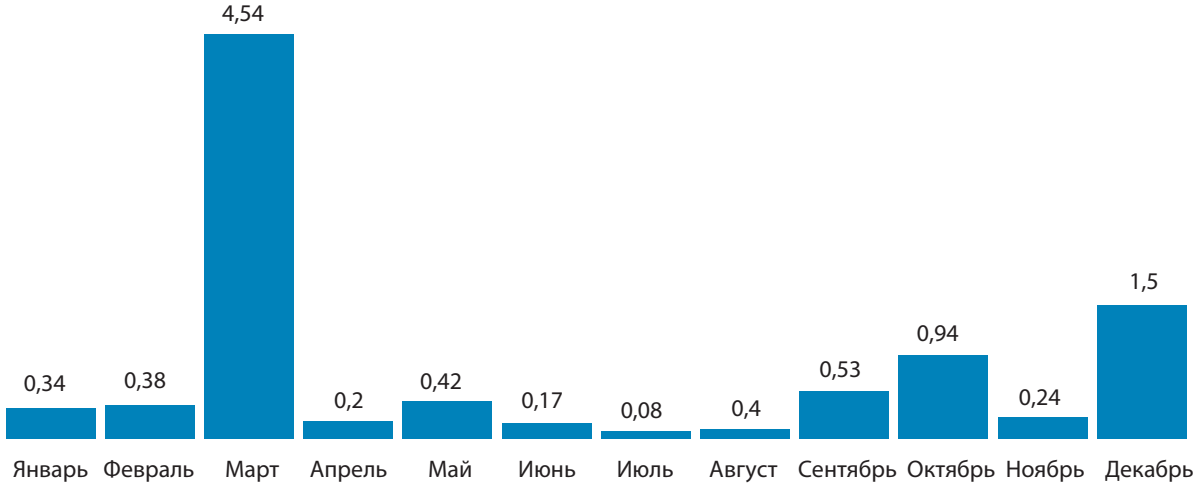


Рис. 4. Средняя интенсивность DDoS-атак (Гбит/с), 2018 год



Средняя длительность DDoS-атак на банки составляет около 14 часов. Мощность DDoS-атак также возросла. Самая серьезная атака в 2018 г. велась с интенсивностью 47 Гбит/с (рекорд 2017 г. – 33 Гбит/с).

Рис. 5. Самые продолжительные DDoS-атаки (часов), 2018 год

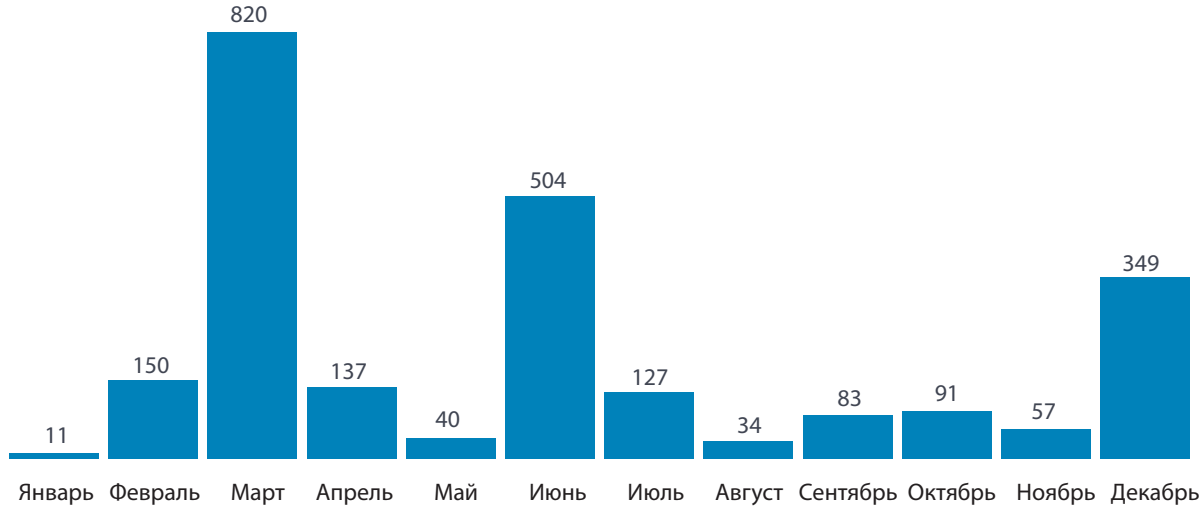
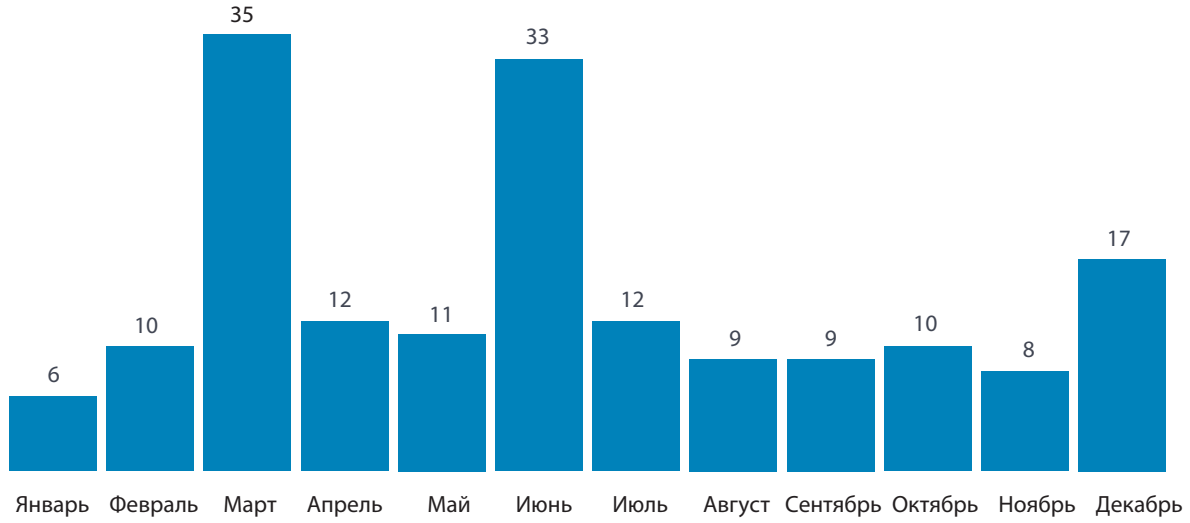


Рис. 6. Средняя продолжительность DDoS-атак (часов), 2018 год



Статистика распределения DDoS-атак по отраслям подтверждает, что эта угроза наиболее актуальна для компаний, чьи критически важные бизнес-процессы зависят от доступности онлайн-сервисов и приложений. К таким компаниям, безусловно, относятся и банки.

Рис. 7. Распределение DDoS-атак по отраслям, 2018 год

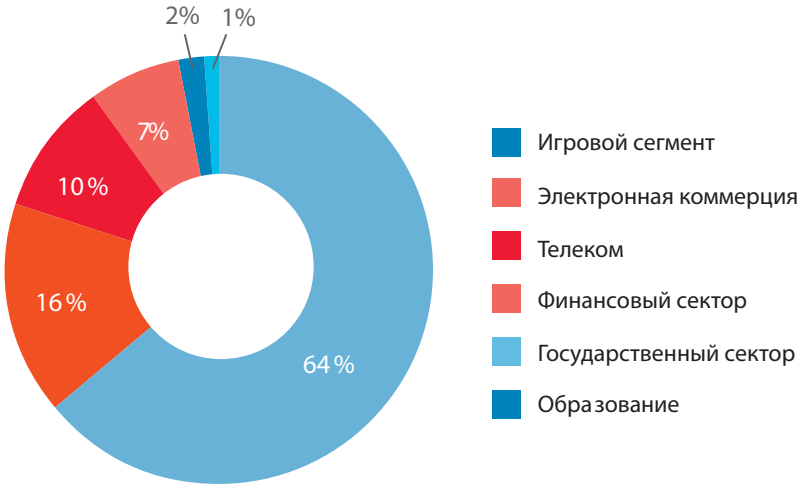
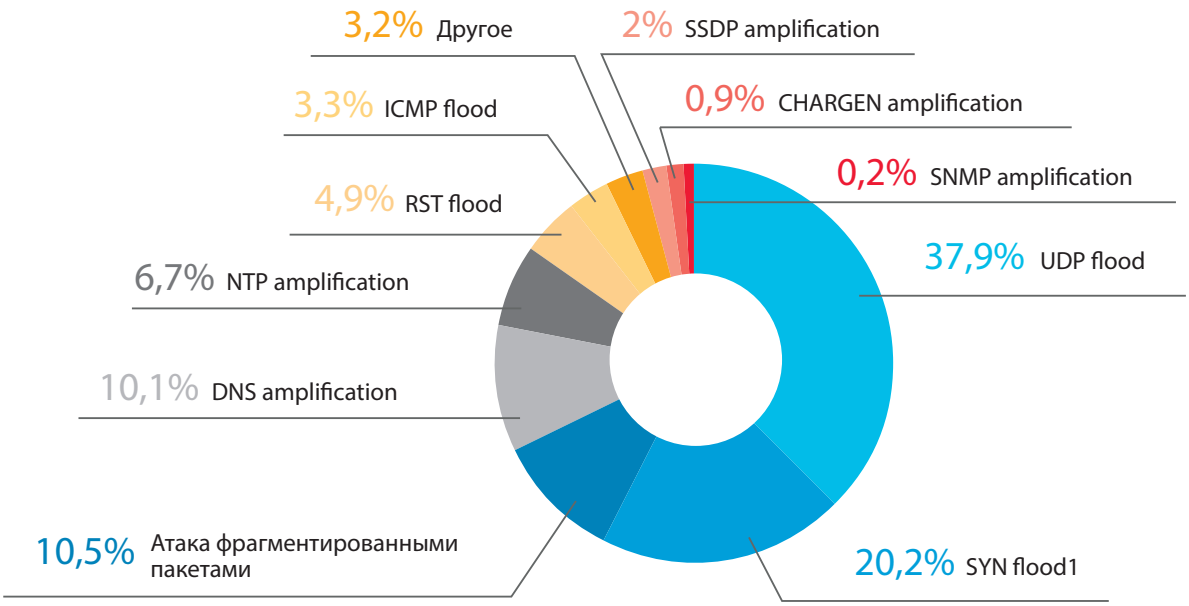


Рис. 8. Распределение DDoS-атак по типам, 2018 год



Отмечается резкий рост доли атак с амплификацией. При организации таких атак злоумышленники отправляют запросы с поддельным адресом источника к серверам, которые отвечают жертве атаки многократно увеличенными пакетами. Этот метод DDoS может выйти на новый виток и стать очень распространенным уже в ближайшее время, поскольку он также не требует затрат на организацию или покупку ботнета.

В то же время одновременно – с развитием Интернета вещей и ростом числа известных уязвимостей IoT-устройств – можно ожидать появления и новых мощных ботнетов, а следовательно, и удешевления услуг по организации DDoS-атак.

ОБЗОР ЗАЩИЩЕННОСТИ ИНФРАСТРУКТУРЫ

Защищенность периметра и внешних банковских сервисов

Данная часть отчета содержит сведения, полученные в результате проведения следующих работ:

- Инструментальная и ручная оценка защищенности внешних сервисов кредитно-финансовых организаций, выполняемая группой анализа защищенности Solar JSOC.
- Проведение расследований, в рамках которых были восстановлены цепочки атак, задействовавшие внешние сервисы, опубликованные в сети Интернет.

Как правило, банки очень внимательно следят за безопасностью внешнего периметра, и нечасто удается найти критичные уязвимости, позволяющие получить доступ к внутренним ресурсам организации простыми методами.

Тем не менее в ходе проектов по анализу защищенности всегда удается обнаружить ряд уязвимостей, позволяющих злоумышленнику так или иначе проникнуть в инфраструктуру. К ним относятся:

- Возможность подбора учетных доменных записей через почтовые сервисы и сервисы удаленного доступа.
- Возможность узнать имена сотрудников через опубликованные на сайте документы (иногда в них содержатся метаданные о ПК пользователя).
- Старые, «забытые» тестовые системы с легко подбираемыми паролями.
- Проблемы с мониторингом событий информационной безопасности, приводящие к тому, что найденные уязвимости или недостатки удается долгое время эксплуатировать, не привлекая внимания сотрудников службы ИБ.

Очень часто полученная информация может использоваться для дальнейших действий внутри периметра организации.

Ключевые тенденции и цифры

- 20% случаев – для атаки используются внешние обслуживающие сервисы (опубликованные порталы внешнего и внутреннего обучения, серверы видеоконференцсвязи и так далее) с невысоким уровнем защищенности. При этом используются классические уязвимости типа SQL-инъекций, позволяющие получить доступ во внутреннюю сеть.
- 70% случаев – злоумышленник может успешно собрать учетные данные через сервисы, доступные на внешнем периметре.
- 80% случаев – злоумышленник может успешно подобрать данные учетных записей в сервисах, доступных на внешнем периметре.
- 90% случаев – организация оставляла доступными из сети Интернет тестовые среды ключевых приложений с пониженным уровнем защищенности, что позволяло успешно преодолеть периметр более чем в половине случаев.
- 15% случаев – проникновение производилось путем получения доступа к сетевому оборудованию на внешнем периметре (роутеры/свитчи).

Защищенность платежных систем (АБС, ДБО)

Все большую популярность среди физических и юридических лиц набирают дистанционные каналы банковского обслуживания. Как следствие, банковские системы ДБО становятся привлекательной мишенью для хакеров. Несмотря на то, что количество критичных уязвимостей, таких как SQL injection, постоянно снижается, атаки на бизнес-логику приложений так или иначе актуальны для каждого банка. Хотя эти уязвимости широко известны, их количество не уменьшается, поскольку их выявление в сложных бизнес-системах обычно требует использования анализаторов исходного кода.

Две самые частые уязвимости, которые мы находим в ходе анализа защищенности ДБО, – это XSS (cross-site scripting) и атаки на бизнес-логику IDOR (insufficient direct object references). С помощью первой уязвимости можно атаковать пользователей системы, с помощью второй очень часто можно получить информацию о счетах клиентов, остатках денежных средств на картах и тому подобном.

Ключевые тенденции и цифры

- Минимальное количество логических уязвимостей (например, позволяющих осуществить атаки класса IDOR), которые мы выявляем в банковских приложениях, – четыре.
- В 20% случаев была возможность построить цепочку логических уязвимостей через IDOR: узнать номер счета и остаток средств на нем, а также перевести деньги на сторонний счет, минуя OTP.
- Уязвимости класса XSS также обнаружены в каждом банковском приложении.

Защищенность систем межбанковского взаимодействия (АРМ КБР, SWIFT)

Одним из ключевых трендов 2015–2017 гг. в атаках на кредитно-финансовые организации была попытка компрометации/подмены платежной информации в рамках подсистем межбанковского взаимодействия (АРМ КБР, в одиночных случаях – SWIFT). Данные атаки реализовывались с использованием различных брешей в системах информационной безопасности банков:

- Передача платежных рейсов осуществлялась через файловые сервера с некорректно настроенными правами доступа и неконтролируемым доступом к файлам, что позволяло злоумышленникам осуществлять компрометацию рейса путем взлома машины ИТ-администраторов.
- Профильные сотрудники (узел связи, расчетный центр и так далее) имели возможность удаленного доступа на АРМ КБР или удаленной корректировки информации рейсов, что позволяло получать доступ к информации без компрометации непосредственно АРМ КБР.
- Между системами межбанковского взаимодействия и сегментами общего пользования отсутствовала сегментация, вследствие чего злоумышленники могли получить сетевой доступ с привилегированной учетной записью непосредственно к АРМ КБР.
- Отсутствие мониторинга событий и инцидентов информационной безопасности в рамках ключевого сегмента межбанковского взаимодействия для оперативного выявления и реагирования на возникающие инциденты.

Методические рекомендации Банка России способствовали существенному снижению количества инцидентов в инфраструктуре межбанковского взаимодействия:

- Более чем в половине кредитно-финансовых организаций было принято решение об отказе от использования промежуточных файловых серверов. Оставшиеся в 80% случаев установили политики безопасности, ограничивающие права доступа к ним, и включили расширенный мониторинг копирования или изменения рейсов. Количество соответствующих инцидентов снизилось на 60%.
- В 80% случаев были предприняты меры по максимальной защите рабочих станций профильных подразделений, включая ужесточение политик безопасности (запрет удаленного доступа, минимизация прав пользователя на рабочей станции, усиление контроля актуальности антивирусной защиты). Количество соответствующих инцидентов снизилось на 50%.
- В 95% случаев проведены работы по изоляции и ужесточению правил работы с АРМ КБР. Количество соответствующих инцидентов снизилось на 80%.

Повышение уровня защищенности подсистемы межбанковского взаимодействия снижает шансы злоумышленников на успешное использование описанных выше векторов и заставляет их искать более сложные и интеллектуальные способы атаки на финансовые системы банка.

Атак на подсистему SWIFT в рамках исследования Solar JSOC выявлено не было. Но стоит отметить, что предыдущий опыт с атаками на системы межбанковского взаимодействия заставляет службы информационной безопасности кредитно-финансовых организаций предпринимать упреждающие шаги по повышению их защищенности без фактических прецедентов на территории Российской Федерации.

ОБЗОР ИНСТРУМЕНТОВ И МЕТОДОВ КИБЕРПРЕСТУПНИКОВ

Цели атак. Ключевые тренды

Данный раздел содержит распределение атак по целям злоумышленника. Определение итоговой цели зависит от действий киберпреступника в инфраструктуре, функциональных возможностей вредоносного ПО, внедренного в компанию, и так далее. В отчете учтены как внешние, так и внутренние атаки.

Ключевые тенденции и цифры

- На 50% по сравнению с первой половиной года выросло количество атак, направленных на получение контроля над инфраструктурой. Злоумышленники стремятся незаметно закрепиться в ней с целью детального исследования и получения как можно более глубокого доступа к информационным и технологическим системам. При этом на старте злоумышленники зачастую используют со-

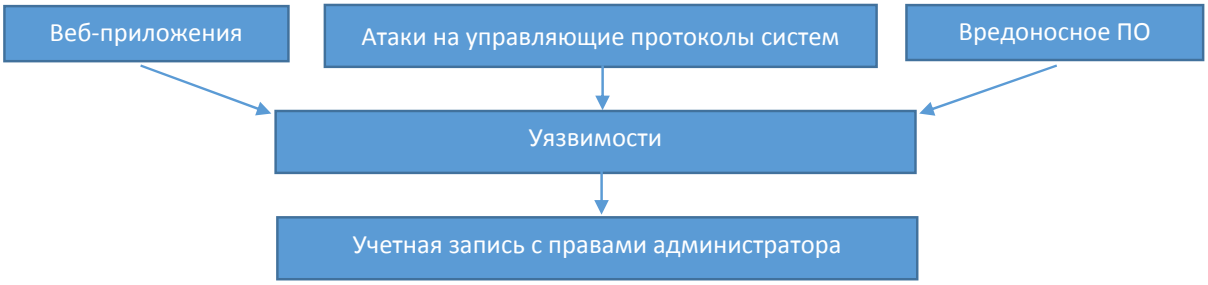
вершенно не профильные инструменты: мы фиксировали случаи рассылки банковских троянов на органы государственной власти и энергетические организации. В дальнейшем управляемые сегменты бот-сети перепродаются другим группировкам и развитие атаки идет уже с помощью специализированного инструментария.

- На 60% относительно первой половины года выросло количество атак, направленных на кражу денежных средств. Однако развитие информационного обмена в рамках сообщества по-прежнему позволяет кредитно-финансовым организациям своевременно получать информацию о способе реализации атаки и препятствовать действиям злоумышленников. Тем не менее фиксируемый рост говорит о том, что атаки будут продолжаться, а инструментарий – постепенно усложняться.
- Во второй половине года аналитики Solar JSOC регулярно сталкивались с вредоносным ПО, оптимизированным для обхода средств защиты, в том числе антивирусов и «песочниц». Также в 2018 г. отмечалась тщательная проработка и усиление «социального» вектора атак. Фишинговые письма становятся все более похожими на привычные рассылки о промоакциях, предстоящих мероприятиях и так далее.

Инструментарий и векторы реализации атак

В качестве самостоятельного объекта исследования мы выделяем атаки, формирующие Kill Chain – последовательность действий злоумышленника, осуществляющего проникновение в информационную систему. Такие атаки не завершаются на этапе получения доступа к конкретной подсистеме, а характеризуются последовательными попытками злоумышленника как можно глубже закрепиться в инфраструктуре и контролировать ее для получения финансовой или иной выгоды.

В 2018 г. аналитики Solar JSOC в 99% случаев сталкивались со следующей общей моделью атаки на кредитно-финансовые организации. После первого проникновения в сеть компании злоумышленник сканирует ее, пытаясь найти уязвимый сервер. Если эксплуатация уязвимости прошла успешно, злоумышленник может в короткие сроки получить доступ и к привилегированным учетным записям сети (технологическим учетным записям, записям ИТ-администраторов), из-под которых в свою очередь добраться до многих объектов инфраструктуры.



В 5% случаев атака злоумышленников начиналась с использования уязвимостей или ошибок конфигурации в управляющих протоколах систем.

Несмотря на то, что ситуация с контролем и инвентаризацией периметра организаций существенно улучшилась, до сих пор можно отметить ряд системных проблем в обеспечении безопасности инфраструктур:

- В **каждой 12-й** организации одно из устройств защиты или телекоммуникационного оборудования имеет опубликованный в Интернете порт управления с дефолтными и/или легко подвергаемыми подбору учетными записями и паролями.
- В каждой организации в среднем раз в месяц появляется **пять** неучтенных или неинвентаризированных сервисов, доступных из Интернета. Обычно это происходит из-за того, что ИТ-специалисты при выполнении работ не консультируются со службой ИБ, в том числе в отношении использования наложенных средств сетевой безопасности для защиты публикуемых сервисов.
- Несмотря на активную борьбу с массовыми атаками в 2017–2018 гг., темпы устранения уязвимостей в кредитно-финансовой сфере остаются невысокими. Среднее время полного закрытия критичной уязвимости составляет около 42 дней, что позволяет злоумышленникам не только разработать соответствующий эксплойт, но и провести несколько атак с его использованием до фактической защиты инфраструктуры. Одной из причин этого является необходимость тестирования корректирующих патчей на разных версиях операционных систем и совместимости со специализированным прикладным ПО. Поэтому для кредитно-финансовых организаций существенную роль играют проработка наложенных или компенсирующих мер по закрытию или выявлению факта использования уязвимости.

В 26% злоумышленники реализовывали первый этап атаки путем компрометации веб-приложения (например, интернет-банка). В случае успеха этот вектор зачастую обеспечивает прямую монетизацию атаки (при компрометации банковских сервисов) без необходимости развивать ее дальше в инфраструктуре. Стоит отметить, что даже массовое использование наложенных средств защиты веб-приложений (Web Application Firewall, WAF) в среднем по отрасли не дает должного эффекта. Высокая динамика выпуска релизов для ключевых банковских приложений и высокие требования к доступности приводят к тому, что политика системы защиты веб-приложений зачастую не успевает пройти полноценное обучение и автоматическую настройку. В результате:

- примерно 40% случаев – политики WAF работают исключительно в режиме мониторинга без активного противодействия атакам;
- 30% случаев – запущены блокировки по частотным сигнатурам, но не производится анализ и профилирование действий пользователей для включения механизма блокирования по белым/черным спискам;

- 25% случаев – включены лишь частные политики блокирования по сигнатурам и профилям.

Наибольшую эффективность в сложившейся ситуации демонстрирует гибридный подход: блокирование и тюнинг максимального количества критичных сигнатур и профилей с активным мониторингом срабатываний всех прочих подозрительных активностей с возможностью оперативного противодействия и блокирования атаки.

Социальная инженерия. Фишинг

Социальная инженерия – обязательная составляющая почти 2/3 всех атак (68%) на банковский сектор, в связи с чем мы решили обратить на него более пристальное внимание.

Ключевые тенденции и цифры

- В среднем каждый шестой пользователь, который не проходит регулярное повышение осведомленности, поддается на приемы социальной инженерии: открывает зараженный файл или отправляет свои данные злоумышленникам. Наиболее подверженные атаке подразделения:
  - юридическая служба;
  - бухгалтерия и финансово-экономическая служба;
  - логистика;
  - секретариат и helpdesk.
- Эффективность фишинга в отношении банковского сектора выше средних значений по рынку во многом потому, что рассылки, ориентированные на банки, обычно лучше подготовлены и продуманы.
- Фишинговые рассылки, ориентированные на банки, на 60% чаще включают персонификацию – обращение к жертве по имени, упоминание реальных рабочих обязанностей сотрудника и так далее. Это повышает уровень доверия к письму, а с ним и вероятность, что сообщение будет открыто.
- Обучение сотрудников основам киберграмотности и регулярная тренировка их навыков существенно влияют на уровень защищенности организаций. Эффективность социальной инженерии снижается практически в два раза: на атаки поддается уже лишь каждый десятый пользователь. Разница в результатах до и после начала обучения и регулярных тренировок сильнее всего заметна у сотрудников финансового и юридического департаментов.

Ключевые тренды развития вредоносного программного обеспечения (ВПО)

В этом разделе мы собрали свои наблюдения и интересные факты о вредоносном программном обеспечении, с которым **JSOC CERT** сталкивался в 2018 – начале 2019 г.:

- Во втором полугодии 2018 г. сменился «лидер» среди ВПО для фишинговых рассылок: троян Dimnie, чаще всего встречавшийся

в первой половине года, уступил место банковскому трояну RTM, таргетированному на российский финансовый сектор.

- С момента, когда аналитики компании ESET впервые рассказали сообществу о трояне RTM, прошло уже два года. За это время он значительно не изменился, а использующие его киберпреступники не внедрили никаких концептуально новых подходов к его распространению.
- Проект Buhtrap, попавший в сеть еще в 2016 г., до сих пор активно используется злоумышленниками. За последние полгода он несколько раз сменил загрузчик (от привычного js до необычного DotNet), легитимное приложение, за счет которого оказывался в памяти (Морской бой, Судоку, Punto Switcher и другие), и не всегда использовал привычный для себя NSIS Installer.
- В сентябре мы зафиксировали использование злоумышленниками нескольких вредоносных библиотек, написанных для легитимных программ удаленного доступа (RMS, TeamViewer). Предназначение библиотек – перехват API-вызовов для сокрытия различных событий, фиксируемых программами (например, удаленного подключения).
- Нельзя не упомянуть и Cobalt. Информация о возможности использования уязвимости CVE-2018-15982 для проведения целенаправленных атак появилась 5 декабря 2018 года. Менее чем через двое суток группировка Cobalt уже рассылала свой downloader, эксплуатирующий эту уязвимость.

Интересные наблюдения 2019 года

- Список самого распространенного вредоносного ПО остался без изменений по сравнению с 2018 годом. В начале 2019 г. специалисты JSOC CERT по-прежнему сталкивались с рассылками Loki Bot, Adwind RAT, FormBook, Scarab, Trickbot, AZORult.
- Продолжались атаки на банки с использованием трояна RTM. Анализ образцов начала 2019 г. показывает, что он был несколько раз модифицирован с целью предотвращения обнаружения и повышения надежности работы. Троян несколько раз менял «оболочку» и получил возможность общения с CnC-серверами, расположенными в сети TOR.
- В течение I квартала 2019 г. фиксировались массовые фишинговые рассылки шифровальщика Troldesh на крупные российские компании. Это была первая в России фишинговая атака, осуществлявшаяся с роутеров, доступных из сети Интернет по административным портам и имевших ненадежные логин и пароль.
- В марте были зафиксированы попытки заражения ряда банков вредоносным программным обеспечением семейства Emotet. Злоумышленники взламывали общедоступные ресурсы с уязвимой версией WordPress, загружали на них вредоносные файлы и затем рассылали по электронной почте ссылки на эти ресурсы.

- Злоумышленники перенимают друг друга лучшие практики. В 2019 г. все чаще используется техника «бесконечного цикла» для обхода средств защиты. При этом загрузчик вредоносного ПО скачивает его на сервер / рабочую станцию не сразу, а через произвольное время. Таким образом, если загрузчик изначально попадает в «песочницу», его вредоносная функциональность остается нераскрытой, а аналитики не могут получить основное тело ВПО для последующего анализа. Эта техника ранее использовалась группировкой Silence, но сейчас постепенно становится более массовым инструментом.
- В 2019 г. стало известно о том, что архив с исходными кодами вредоносного программного обеспечения группировки Carbanak/Fin7 лежит на сервисе VirusTotal с 2017 года. Сам архив можно использовать как инструкцию для тех, кто занимается или хотел бы заниматься разработкой вредоносного кода. Поэтому можно сделать вывод, что изучением хорошо документированного кода начали заниматься не только специалисты по информационной безопасности, но и их противники.
- Между тем сама группировка Fin7 не прекратила свои атаки на банковский сектор. Злоумышленники обновили свой арсенал и сейчас используют модули вредоносного программного обеспечения, написанные на языке JavaScript, распространяя его с помощью фишинговых писем с высочайшим уровнем подготовки. При этом в начале 2019 г. группировка пока обходила стороной российские организации. Но с учетом истории, репутации и уровня подготовки Fin7 необходимо всегда быть готовыми к новой атаке.

Выявление атаки злоумышленников с помощью сбора и анализа информации об угрозах (Threat Intelligence)

Источники Threat Intelligence (TI), используемые в Solar JSOC, можно условно разделить на следующие категории:

- Opensource – открытые базы индикаторов вредоносного ПО, серверов управления и фишинговых ссылок.
- Reputation feeds – платные подписки на репутационные списки вредоносного ПО, серверов управления и фишинговых ссылок.
- APT/IoC reporting – платные подписки на подробные описания 0day вредоносных тел, включающие в том числе описание используемых уязвимостей и хостовые индикаторы вредоносного ПО.
- Information Exchange – информация, полученная в рамках информационного обмена с государственными, ведомственными и иностранными центрами реагирования на инциденты (CERT).
- Internal Solar JSOC database – индикаторы, полученные в результате собственных исследований Solar JSOC или расследований инцидентов.
- User Experience – информация, полученная напрямую от пользователей клиентов (успешное противодействие социальной инженерии, детектирование фишинговых рассылок и тому подобное).

Далее приведена статистика по использованию различных источников Threat Intelligence в детектировании инцидентов.

Рис. 9. Доля инцидентов, детектированных с помощью различных источников Threat Intelligence

Источник	% от общего количества инцидентов, детектированных с помощью TI
1. Opensource	8,9%
2. Reputation feeds	20,8%
3. APT/IoC reporting	18,8%
4. Information Exchange	20,9%
5. Internal Solar JSOC database	20,8%
6. User Experience	9,8%

Статистика показывает, что доля специализированных «отраслевых» индикаторов в кредитно-финансовой сфере очень велика. Вследствие этого использование данных о кибератаках, поступающих в рамках информационного обмена (в том числе в рамках ФинЦерт) и от внутренних исследований крупных сервис-провайдеров, имеющих существенную клиентскую базу в отрасли, представляется наиболее эффективным.

Информационное взаимодействие с ФинЦЕРТ

За 2018 г. командой Solar JSOC был получен 51 информационный бюллетень от ФинЦЕРТ. По результатам их обработки команда Solar JSOC собрала следующую статистику:

- Сетевые индикаторы были обнаружены по 28 бюллетеням в 20 компаниях (одни и те же индикаторы встречались в нескольких компаниях), причем 22 случая были определены как подтвержденные инциденты с проведением дальнейших расследований.
- Хостовые индикаторы были обнаружены по 10 бюллетеням в 8 подключенных компаниях, причем только 3 случая определены как ложные срабатывания.

Результаты верификации индикаторов говорят о существенном улучшении их качества и релевантности для использования в задачах мониторинга и реагирования на инциденты информационной безопасности.

Из выявленных и подтвержденных инцидентов в трех случаях оперативное взаимодействие команды Solar JSOC с клиентом позволило существенно минимизировать ущерб. Во всех остальных случаях совместное реагирование со службой клиента дало возможность полностью предотвратить ущерб от возникшего инцидента.

Стоит отметить, что система АСОИ ФинЦЕРТ позволила достичь существенного ускорения выявления и реагирования на кибератаки в банковской сфере. Положительный эффект достигается как за счет появления

машиночитаемой информации об индикаторах с возможностью полуавтоматизированной загрузки в системы выявления и анализа событий, так и за счет автоматизированного взаимодействия подсистем и контрагентов без задержки передачи данных, свойственной почтовым каналам. Сообщество рассчитывает, что дальнейшее развитие подсистемы позволит еще больше сократить время от фактической реализации первой атаки до автоматизированного реагирования и превентивного противодействия инцидентам.

РЕКОМЕНДАЦИИ SOLAR JSOC

Статистика и анализ киберугроз свидетельствуют о том, что полноценная эксплуатация, качественная настройка даже базовых средств защиты, а также реализация основных организационных мер способны серьезно повысить уровень информационной безопасности организации. Особое внимание при этом следует уделять следующим аспектам:

- **Инвентаризация внешнего периметра.** Результаты тестов на проникновение в банковском сегменте показывают, что большинство кредитно-финансовых организаций оставляют доступными из сети Интернет различные элементы инфраструктуры: тестовые среды ключевых приложений, уязвимое сетевое оборудование, серверы с устаревшим ПО и так далее. Все это облегчает задачу злоумышленника по проникновению в инфраструктуру.
- **Информационный обмен.** Участие в системах информационного обмена о новых способах атак, видах вредоносного ПО и уязвимостях не требует финансовых затрат и при этом предоставляет возможность раннего и даже превентивного реагирования на киберугрозы.
- Настоятельно рекомендуется **создание центров мониторинга и реагирования на кибератаки** (или привлечение внешних сервисов). Стремительная динамика возникновения новых методов атак и модификации старых, растущая доля атак, производимых в ночное время и выходные дни, размывание периметра, низкий уровень киберграмотности пользователей – все это приводит к тому, что при обеспечении безопасности нельзя полагаться исключительно на средства защиты как таковые. Инфраструктура часто атакуемых организаций, к которым, без сомнения, относятся банки, нуждается в постоянном и круглосуточном мониторинге с возможностью оперативного реагирования на возникающие инциденты информационной безопасности.

Также для защиты от внешних кибератак рекомендуется:

- **Обеспечить защиту веб-сервисов.** Повышение уровня защищенности подсистем межбанковского взаимодействия вынуждает злоумышленников искать другие способы атаки на банки. Вследствие этого фокус внимания киберпреступников смещается в сторону банковских веб-приложений: каждая четвертая сложная целенаправленная атака на банк использует этот вектор в качестве первого этапа.

- **Реализовать контроль защищенности исходного кода** банковских мобильных и веб-приложений. На данном этапе большинство исследованных банковских приложений содержат те или иные уязвимости, в том числе позволяющие узнать номер счета клиента и остаток средств на нем, а также перевести деньги на сторонний счет, минуя OTP. В связи с этим банкам рекомендуется контролировать защищенность исходного кода мобильных и веб-приложений еще на этапе разработки. Системный подход к защите приложений подразумевает внедрение методики Secure Software Development Lifecycle (SSDLC), суть которой состоит в том, что при создании банковских приложений требования безопасности должны учитываться наравне с требованиями функциональности и отказоустойчивости. Применение технологий статического анализа позволяет снизить риски вывода средств из банков путем атаки на пользовательские приложения.
- **Обеспечить защиту от DDoS-атак.** Рост количества и интенсивности DDoS-атак диктует необходимость в использовании соответствующих сервисов защиты. Рост сегмента IoT приводит к упрощению создания ботнетов, параллельно растет число DDoS-атак, вовсе не требующих применения бот-сетей. Все это позволяет предположить, что данный вектор атак в ближайшее время не утратит актуальности.
- Периодически проводить **анализ уровня защищенности и тестирования на проникновение**. Несмотря на достаточно высокий средний уровень ИБ в финансово-кредитных организациях, практически каждое тестирование на проникновение оказывается успешным. Периодическое проведение анализа защищенности и применение на практике рекомендаций, полученных по результатам тестирования, позволит устранить уязвимости, которыми киберпреступники могут воспользоваться для совершения атаки.