Ростелеком
Солар

Отчет Solar JSOC об актуальных киберугрозах в финансовом секторе за 2021 – начало 2022 года

rt-solar.ru

ОГЛАВЛЕНИЕ

О компании

«Ростелеком-Солар», компания группы ПАО «Ростелеком», – национальный провайдер сервисов и технологий для защиты информационных активов, целевого мониторинга и управления информационной безопасностью. В основе наших технологий лежит понимание, что настоящая информационная безопасность возможна только через непрерывный мониторинг и удобное управление системами ИБ. Этот принцип реализован в продуктах и сервисах «Ростелеком-Солар». Solar JSOC – первый российский центр мониторинга и реагирования на кибератаки, лидер российского рынка Security Operations Center (SOC).

Список сервисов Solar JSOC:

- Мониторинг и анализ инцидентов ИБ
- Эксплуатация систем ИБ и реагирование на атаки
- Анализ угроз и внешней обстановки
- Комплексный контроль защищенности
- Реагирование на инциденты и техническое расследование
- Построение SOC или его частных процессов (в том числе центров ГосСОПКА)

Совокупно Solar JSOC обеспечивает контроль и выявление инцидентов для:

- **около 200** крупных организаций (общей численностью свыше 600 тыс. сотрудников) из разных отраслей экономики: банки, энергетика и нефтегаз, органы государственной власти и др.
- **более 2 тыс.** внешних сервисов, опубликованных в интернете;
- **более 95 тыс.** серверов общего, инфраструктурного и прикладного назначения.

Введение

2021 год можно смело назвать одним из самых насыщенных с точки зрения количества обнаруженных критических 0-day-уязвимостей. Ввиду широкой популярности сервисов, библиотек и ПО, в которых были обнаружены уязвимости, под угрозой оказались сразу все отрасли экономики.

При этом финансовый сектор остается особенно привлекательным для злоумышленников. Именно в 2021 году произошла первая за 3 года успешная атака на российский банк. Ущерб от нее был оценен в 500 млн рублей.

Основной угрозой для отрасли являются высокопрофессиональные хакерские группировки, так как периметр банков и других крупных финансовых организаций обычно хорошо защищен и для его взлома нужна техническая подкованность и серьезные финансовые вложения. По этой же причине злоумышленники более низкой квалификации вынуждены направлять свои атаки на клиентов банков, применяя к ним различные методы социальной инженерии.

В рамках данного отчета мы сфокусировались на обзоре инцидентов, зафиксированных с начала 2021 года, особо уязвимых элементах защиты инфраструктуры и разобрали наиболее популярные ВПО, используемые злоумышленниками при атаках на финансовый сектор. Также мы сравнили финансовый сектор с другими отраслями экономики с точки зрения их готовности к хакерским атакам.

Ключевые выводы

Свыше **60%** атак в отчетном периоде пришлось на фишинг.
При этом растет популярность фишинга по сервисной модели, то есть когда кибергруппировка заказывает разработку фишинговой рассылки у других хакеров, которые на этом специализируются.

В **72%** организаций финансового сектора обнаружен факт компрометации учетных записей.

В отчетном периоде наибольшее число инцидентов в финансовом секторе было зафиксировано в Краснодарском и Красноярском крае, Бурятии, Иркутской области и на Алтае.

Методология

Представленная в отчете информация основывается на:

- аналитике инцидентов и атак, выявленных командой Solar JSOC в рамках оказания услуг мониторинга и реагирования на кибератаки;
- результатах расследований инцидентов, проводимых командой Solar JSOC CERT;
- агрегированных данных об атаках и вредоносном ПО, собираемых сетью ловушек (honeypot) и сенсоров, размещенных на сетях связи и в центрах обработки данных по всей России;
- данных, получаемых в рамках коммерческих подписок от вендоров и партнеров и информационного обмена с российскими и зарубежными CERT.

Финансовый сектор включает как банки, так и страховые компании.

О модели уровней нарушителей

Очевидно, что при выборе решений для защиты от внешних и внутренних злоумышленников эффективнее всего будет начать с определения профиля атакующего: каков уровень его подготовки, какие средства и тактики могут использовать хакеры. Но как заранее понять, придется ли службе ИБ противостоять шаблонным автоматизированным атакам ботнетов или стоит готовиться к атакам профессиональных хакерских группировок?

Накопив огромный опыт в противостоянии злоумышленникам самых разных уровней, мы обнаружили определенные сходства и различия в подходах к атакам, более того, сходства касались не только выбора методик и тактик, но и целей атак. На основании этих данных мы построили «модель уровней злоумышленников», которая легла в основу наших исследований. Согласно данной модели всех атакующих можно разделить на пять основных категорий:

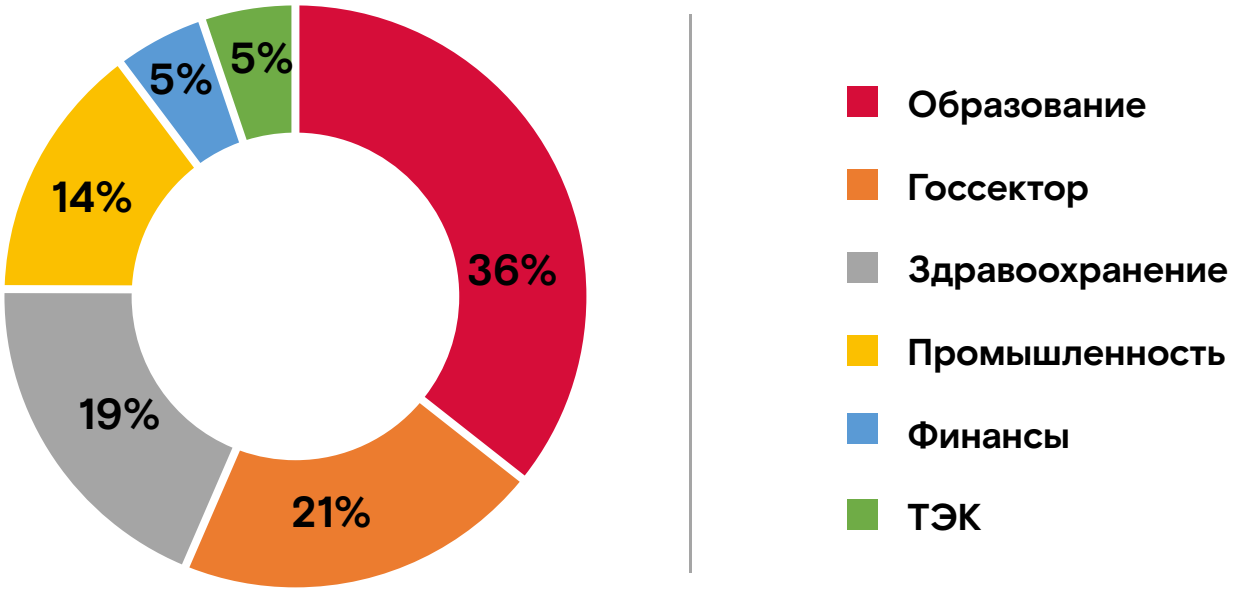
Категория нарушителя	Типовые цели	Возможности нарушителя	Защитные меры
Автомати-зированные системы	Взлом устройств и инфраструктур с низким уровнем защиты для дальнейшей перепродажи или использования в массовых атаках	Автоматизированное сканирование	Установить и настроить UTM и WAF, задать правило о своевременной установке патчей и обновлений
Киберхулиган/ Энтузиаст-одиночка	Хулиганство, нарушение целостности инфраструктуры	Официальные и open-source-инструменты для анализа защищенности	Установить и настроить антивирус, антиспам, UTM и WAF, задать правило о своевременной установке патчей и обновлений. Анализировать журналы аудита СЗИ
Киберкриминал / Организованные группировки	Приоритетная монетизация атаки: шифрование, майнинг, вывод денежных средств	Кастомизированные инструменты, доступное ВПО, доступные уязвимости, социальный инжиниринг	Добавить к базовым средствам защиты инструменты непрерывного мониторинга и реагирования и анализаторы периметрового трафика или подключить коммерческий SOC. Повышать киберграмотность сотрудников

Категория нарушителя	Типовые цели	Возможности нарушителя	Защитные меры
Кибернаемники / Продвинутые группировки	Нацеленность на заказные работы, шпионаж в интересах конкурентов, последующая крупная монетизация, хактивизм, деструктивные действия	Самостоятельно разработанные инструменты, приобретенные 0-day-уязвимости	Дополнить базовые средства защиты продвинутыми решениями (Anti-APT, Sandbox, контроль технологических сегментов). Подключить продвинутый инструментарий SOC, включая EDR и NTA. Также нужна глубокая аналитика регистрируемых событий для выявления взаимосвязи между инцидентами
Кибервойска / Прогосударственные группировки	Кибершпионаж, полный захват инфраструктуры для возможности контроля и применения любых действий и подходов, хактивизм	Самостоятельно найденные 0-day-уязвимости, разработанные и внедренные «закладки»	Необходим весь доступный спектр инструментов и сервисов, высокая зрелость ИТ- и ИБ-инфраструктуры, а также качественная экспертиза для выявления неочевидных аномалий на сети и хостах и процессов. Использовать маппинг по Killchain+Mitre ATT&CK для выявления цепочек взаимосвязей между инцидентами

Кто атакует банки и финорганизации?

Нападения на банки со стороны киберхулиганов и злоумышленников со средней квалификацией происходят крайне редко. А поскольку именно такие массовые атаки составляют большую часть киберинцидентов, то доля финсектора в общей статистике невелика:

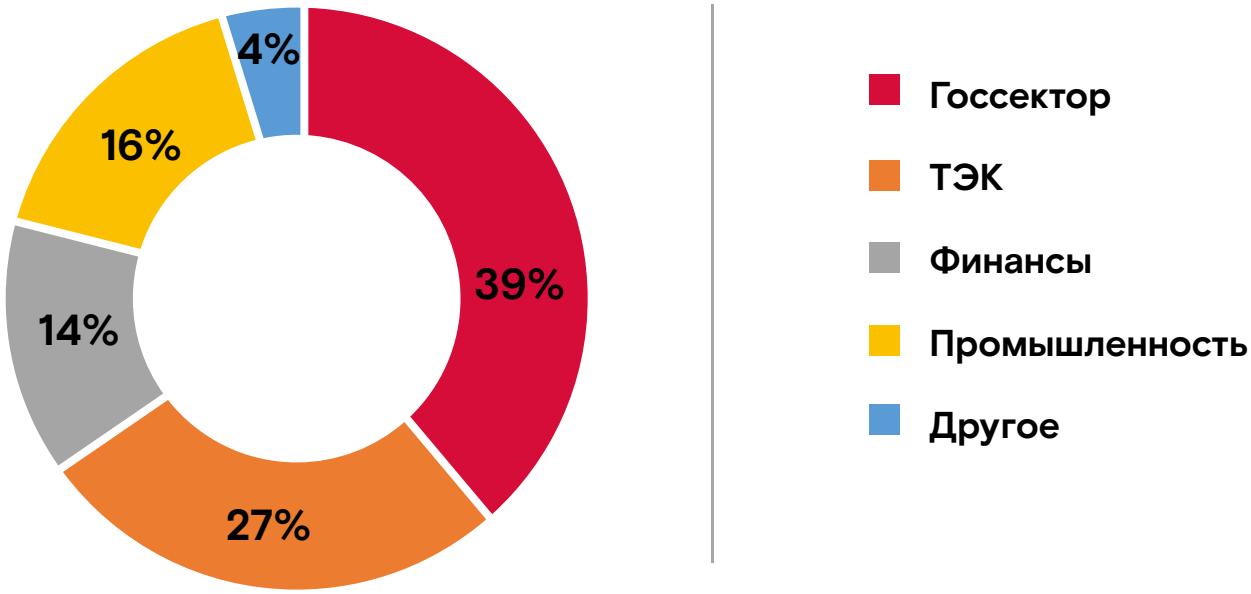
Распределение атак по отраслям



Это в первую очередь связано с высокой защищенностью внутреннего периметра. Повышение сложности применяемых хакерами тактик и инструментов, ужесточение контроля со стороны регуляторов, миграция бизнес-процессов в онлайн формируют высокие требования к безопасности организаций, предоставляющих финансовые услуги. В итоге, даже если хакерам удается совершить успешную фишинговую атаку или воспользоваться скомпрометированными учетными записями, ИБ-команда достаточно быстро обнаруживает попытки «шаблонного» вторжения.

Доля киберинцидентов, связанных с профессиональными хакерами, в финансовом секторе выше:

Распределение APT-атак по отраслям



Таким образом, несмотря на защищенность перед автоматизированными системами и киберхулиганами, банки и другие финансовые организации более уязвимы перед высококвалифицированными злоумышленниками, которые используют более сложные техники и способны долго оставаться незамеченными в инфраструктуре. Подтверждением этого может служить нашумевшая атака на банк через систему межбанковских переводов АРМ КБР (автоматизированное рабочее место клиента ЦБ). Сначала хакеры скомпрометировали одно из рабочих мест аффилированной с банком компании. Далее они получили доступ к внутренней сети учреждения и начали искать в ней доступные уязвимости. На это у них ушло примерно полгода. Наконец в январе 2021 года группировка похитила цифровые ключи и позже использовала их для подписания платежей, проходящих через транспортный шлюз ЦБ. Таким образом, хакеры смогли перевести деньги из атакованного банка на собственный счет. По разным оценкам, ущерб составил около 500 млн руб.

Однако эта атака стала единственным крупным инцидентом в финансовой сфере за последнее время. В целом же число атак продвинутых группировок на российские банки сокращается. Это связано с тем, что основная цель при атаке на финорганизации – монетизация за счет вывода средств со счетов. Но за последние годы уровень информационной безопасности финансовой отрасли, особенно крупных банков, в России значительно вырос, что обусловлено в первую очередь жесткими требованиями в этой части со стороны ЦБ. Поэтому профессиональные хакеры ищут другие способы обогащения: за счет кибершпионажа, хищения корпоративных данных, захвата инфраструктуры, компрометации данных топ-менеджеров. Для прямой монетизации профессиональные злоумышленники все чаще ищут банки в других странах, к которым не везде предъявляются такие жесткие требования, как в России.

Как атакуют банки и финорганизации?

Фишинг как сервис

В 60% атак в отчетном периоде для проникновения в инфраструктуру хакеры использовали фишинг. При этом не у всех злоумышленников есть возможность подготовить эффективную таргетированную фишинговую рассылку, особенно если хакеры не являются носителями русского языка. В то же время у нарушителей, обладающих большим опытом в подготовке таргетированного фишинга, не всегда хватает навыков для того, чтобы закрепиться в инфраструктуре, не говоря уже о продвижении внутри хорошо защищенной инфраструктуры банка. Поэтому все чаще первые заказывают фишинг у вторых, получая эту «услугу» как сервис.

Такой подход приводит к снижению стоимости атаки для хакеров, ведь содержать в группировке несколько высококвалифицированных специалистов, владеющих русским языком, значительно дороже, чем прибегнуть к сервисной модели. Скорее всего, в обозримом будущем спрос на подобный сервис будет только расти, что приведет к увеличению числа фишинговых атак на финансовый сектор. Уже сейчас виден явный рост числа объявлений с предложением фишинговых услуг в даркнете и теневых Telegram-каналах.

Компрометация учетных записей

В 72% организаций финансового сектора установлен факт компрометации учетных записей. Их утечка наряду со случайной публикацией этих данных в исходном коде в публичных репозиториях является наиболее распространенной проблемой для отрасли. С одной стороны, это говорит о том, что рядовые сотрудники используют адрес своей рабочей почты на фишинговых ресурсах. С другой – сами разработчики прописывают свои учетные данные в коде, чтобы при программировании каждый раз не заполнять логин и пароль, а публикуя код, например, на GitHub, просто забывают, что пароль там прописан в явном виде.

Проблема обострилась с началом пандемии, когда многие работники перешли на удаленный режим работы, который большинство организаций сохраняет до сих пор. В таких условиях удаленное подключение злоумышленников с неизвестного IP-адреса может выглядеть вполне легитимным для ИБ-службы, а дальнейшее обнаружение будет зависеть напрямую от квалификации как безопасников, так и атакующих. А если в организации нет двухфакторной аутентификации, то компрометация учетной записи и дальнейшее проникновение хакера во внутреннюю инфраструктуру практически гарантировано.

Распространенные инструменты атакующих

- Наиболее популярные средства удаленного администрирования, загружаемые хакерами, это: **ammyyrat** (использовался в 30% атак) и **rmsrat** (18% атак).

- В качестве утилит по догрузке ВПО и их модулей чаще всего использовалась вредоносная программа Bitser (29% атак). Bitser загружает вредоносное программное обеспечение с помощью службы Windows BITS (Background Intelligent Transfer Service), которая отвечает за передачу файлов между клиентом и сервером.

- Среди банковских троянов, актуальных для операционной системы Android, наиболее популярным оказался **android.remotecode** в различных модификациях, его доля среди остальных android-троянцев составила 22%.

Профессиональные APT-группировки редко прибегают к использованию готовых утилит для проведения атаки. Обычно у каждой команды есть собственные разработки, тем не менее среди всех зафиксированных инструментов можно выделить следующие популярные утилиты и ВПО:

Cobalt Strike – продукт, используемый атакующими для эксплуатации и постэксплуатации уязвимостей (8% от всего ВПО, используемого профессиональными хакерами).

FormBook – шпионское ВПО, широко известное с 2016 года. Его функционал позволяет регистрировать нажатия клавиш, похищать содержимое буфера обмена, извлекать данные из http-соединения. Чаще всего распространяется через фишинговые письма (доля составила 4%).

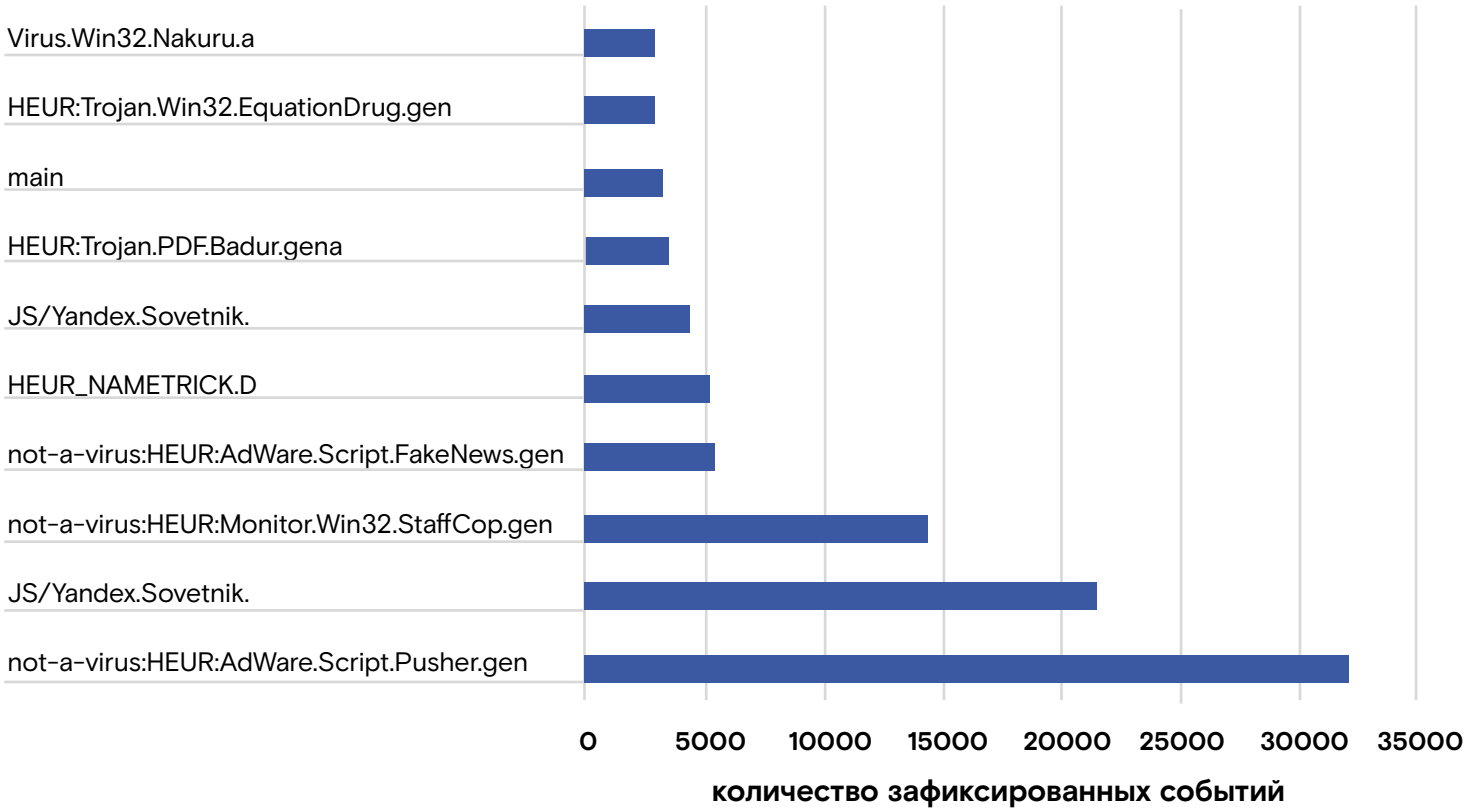
Noon – шпионское ВПО, широко известное с 2016 года. Его функционал позволяет регистрировать нажатия клавиш и похищать пароли из браузера (доля составила 4%).

Quasar – RAT, используется злоумышленниками для удаленного контроля над скомпрометированными компьютерами сотрудников (доля составила 3%).

Penguish – ВПО, используемое злоумышленниками для загрузки других малварей (доля составила 3%).

Малвари, обнаруженные во внутреннем периметре

На внутреннем периметре банков чаще всего антивирусное ПО обнаруживало следующие малвари:



Распространенные недостатки ДБО

При анализе защищенности мобильных приложений банков во всех проектах были обнаружены недостатки и уязвимости, которые потенциально могли привести к финансовым потерям. Ниже представлено описание уязвимостей и недостатков, с которыми команда Solar JSOC встречалась чаще всего.

- **Некорректная реализация алгоритма округления сумм транзакций.** Это возможно, когда хакер находит ошибку в бизнес-логике приложения. Например, при покупке валюты сумма округляется до сотых долей. Данный недостаток позволял приобрести 1 цент США за 38 копеек, т. е. купить валюту по курсу в 38 рублей за 1 доллар США. Потенциальный злоумышленник мог бы автоматизировать проведение подобных операций и получить дополнительные денежные средства, что привело бы к финансовому и репутационному ущербу банка.

- **Небезопасные прямые ссылки на объекты.** В части приложений отсутствовало эффективное разграничение прав доступа при обращении к внутренним объектам. Данная уязвимость может привести к получению несанкционированного доступа к чувствительной информации пользователей, а также информации, имеющей ценность для злоумышленников при проведении дальнейших атак. Например, учетные данные администратора, данные о сервере или версии используемых сервисов.

- **Отсутствие ограничения при отправке СМС-сообщений с кодом подтверждения операции.** В приложениях отсутствовали ограничения на количество совершаемых запросов для отправки кодов подтверждения на мобильный номер пользователя. В результате чего появлялась возможность отправки множества сообщений на один номер телефона в короткий промежуток времени. Таким образом, злоумышленники могут сколько угодно долго подбирать подходящий пароль от системы, и эти попытки не будут блокироваться. Данный недостаток позволяет обойти установленные в приложении ограничения и может привести к серьезным финансовым потерям.

- **Получение информации о клиенте по номеру телефона.** При денежном переводе по номеру телефона или карты на сервер отправлялся запрос для получения информации о получателе. При этом в ответе на данный запрос содержались полные Ф. И. О. клиента, хотя в мобильном приложении отображались сокращенная фамилия и полные имя и отчество. Таким образом, потенциальный злоумышленник мог бы получить список мобильных телефонов клиентов банка, а затем и их Ф. И. О. Подобная информация, например, позволяет проводить социотехнические атаки на пользователей. А любая атака на пользователей наносит банку репутационный ущерб и снижает лояльность клиентов.

Статистика фактов компрометации по регионам

Ниже представлены ТОП-5 регионов, где в отчетный период было зафиксировано наибольшее количество фактов компрометации инфраструктуры финансовых организаций:

7%	от общего числа инцидентов в отрасли	Красноярский край
6%	от общего числа инцидентов в отрасли	Краснодарский край
5%	от общего числа инцидентов в отрасли	Республика Бурятия
5%	от общего числа инцидентов в отрасли	Алтайский край
5%	от общего числа инцидентов в отрасли	Иркутская область

Потенциальные последствия атаки

Успешная кибератака на финансовую организацию может привести как к денежным, так и к репутационным потерям. Однако определить окончательный размер ущерба от кибератаки можно лишь по завершении отчетного периода, то есть как минимум финансового года. Более репрезентативный результат можно получить, сравнив показатели двух пятилетних периодов, глубоко проанализировав динамику и тенденции каждого из них, – ведь последствия кибератаки в их финансовом эквиваленте растягиваются в среднем на 3–4 года.

Сумма потерь зависит от масштаба финансовой организации и от типа самой атаки. Если речь идет о социальной инженерии, направленной на клиентов банка и реализуемой злоумышленниками со средней квалификацией, то потери могут начинаться от нескольких тысяч рублей. При этом такие атаки сильно ударяют по репутации, так как потерявший деньги клиент может отказаться от услуг банка, предать факт хищения публичной огласке и попытаться получить компенсацию через суд. Такие негативные сообщения могут ассоциироваться у людей с ненадежностью финансовой организации и привести к оттоку клиентов.

Ущерб от таргетированных атак может достигать десятков миллиардов рублей. По разным оценкам, годовая прибыль организации может пострадать на 10–11% в результате действий профессиональных хакеров. Более подробно об экономике киберинцидента на финансовый сектор можно прочитать в нашем предыдущем отчете.

Ростелеком
Солар

rt.ru
rt-solar.ru

solar@rt-solar.ru
+7 (499) 755-07-70