Киберугрозы финансовой отрасли: промежуточные итоги 2023 года

Positive Technologies

ptsecurity.com

Содержание

По данным Центрального банка России, в первой половине года злоумышленники украли с банковских счетов и карт россиян порядка 4,5 млрд рублей. Объем похищенных средств непрерывно растет не первый год, а в 2023-м увеличился почти на 30% по сравнению со средними показателями 2022 года. Если говорить о потерях самих банков из-за действий киберпреступников, то в прошлом году ущерб оказался незначительным. За первые три квартала этого года мы также не наблюдали каких-либо громких инцидентов с хищением средств с корреспондентских счетов кредитных организаций в России, но подобные случаи происходили за рубежом. Например, хищение миллионов долларов из индийского Mahesh Bank, уровень защищенности которого оставлял желать лучшего. Слабозащищенные организации и клиенты банков сегодня являются наиболее популярными мишенями для злоумышленника. Это лишь один из трендов, остальные будут рассмотрены далее.

Мы продемонстрируем факторы, которые задают актуальные тренды киберугроз для финансовых организаций сегодня, а также проанализируем интересы самих преступников на основе объявлений, размещенных на теневых площадках дарквеба и в специализированных телеграм-каналах[1]. Аналитика основана на собственной экспертизе компании Positive Technologies, а также на данных из внешних авторитетных источников[2] за первые три квартала года. В выборку организаций включены не только банки, но и некредитные финансовые организации (например, страховые компании, профессиональные участники рынка ценных бумаг, инвестиционные фонды).

[1] В ходе исследования мы проанализировали 236 телеграм-каналов и форумов в дарквебе с общим количеством пользователей 16 734 680 и общим числом сообщений 112 812 462. В выборку попали крупнейшие разноязычные площадки с разной тематической направленностью.

[2] В качестве внешних источников использовались аналитические отчеты ведущих компаний, обладающих собственной экспертизой в кибербезопасности, а также новостные источники, агрегирующие информацию о киберинцидентах, федеральные новостные агентства. Ссылки на некоторые такие источники, чью информацию мы использовали для примеров, указаны в тексте.

Тренды киберугроз в финансовом секторе

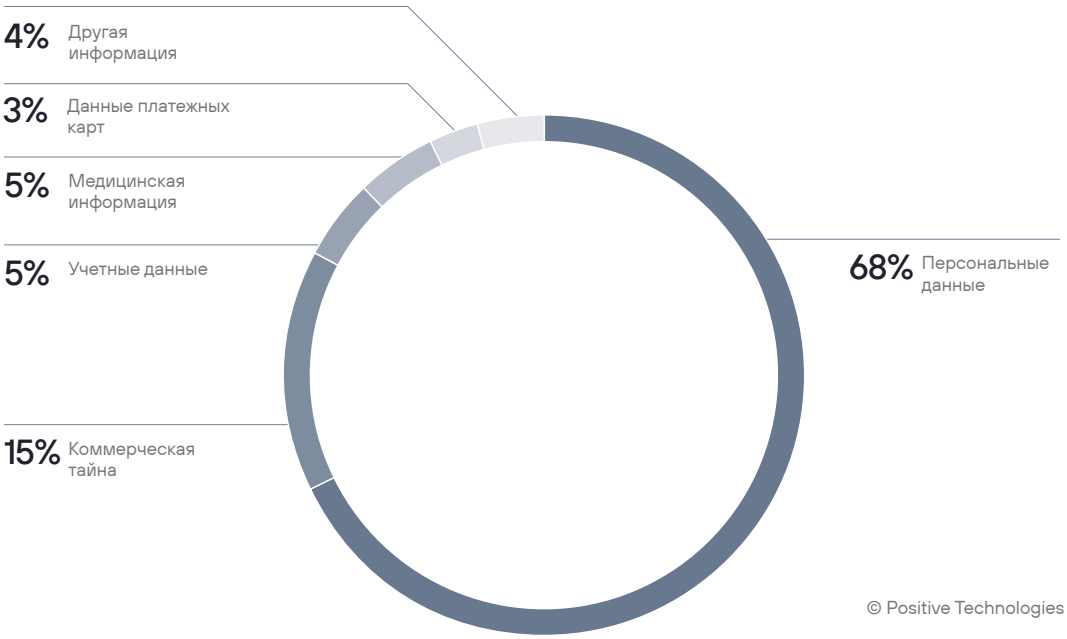
По нашим данным, количество успешных кибератак в финансовом секторе год от года растет. В третьем квартале 2023 года мы зафиксировали вдвое больше уникальных киберинцидентов, чем в аналогичном периоде годом ранее. Это говорит о пристальном внимании преступников к отрасли.

Среди последствий атак выделяются утечки данных (64%), остановка работы отдельных сервисов или ключевых бизнес-процессов (40%). Подобные выводы мы делали и в прошлогоднем исследовании, тогда доля утечек составляла 51%, а нарушение основной деятельности компании возникало в результате 42% инцидентов. Эта тенденция объяснима: сложные атаки на хорошо защищенные финансовые организации с целью кражи денег стали редким явлением на фоне роста более простых в реализации атак вымогателей и крупных утечек данных клиентов. Злоумышленники сегодня не только продают базы данных, но и раздают их бесплатно, таким образом наказывая организации за отказ от уплаты выкупа. Стоимость таких баз и распространенность предложений о продаже и покупке на теневых площадках рассмотрены в следующем разделе.

Рисунок 1. Последствия успешных атак на финансовые организации (Q1–Q3 2023)

Подавляющее большинство утечек содержат персональные данные клиентов и коммерческую информацию организаций. Кроме того, среди утечек нередко можно обнаружить номера платежных карт и учетные данные, в утечках страховых компаний присутствует медицинская информация (специальная категория персональных данных в России).

Рисунок 2. Типы украденных данных в успешных атаках на финансовые организации (Q1–Q3 2023)

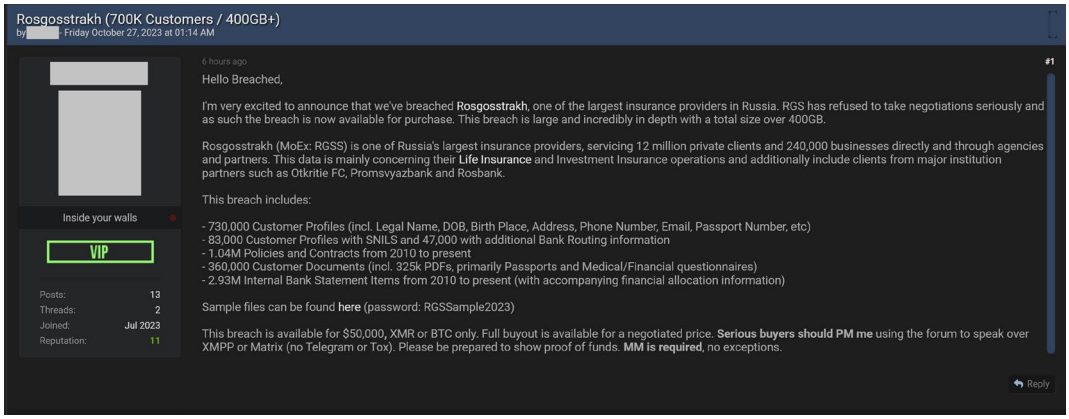


Так, в октябре Роскомнадзор подтвердил факт утечки персональных данных около одного миллиона клиентов МТС Банка, в которой содержались среди прочего Ф. И. О., номера телефонов, ИНН, даты рождения, частично номера банковских карт граждан. А несколькими месяцами ранее «Ренессанс страхование» подверглась кибератаке, в результате которой преступники получили доступ к примерно 2% клиентской базы. По данным телеграм-канала «Утечки информации», в сети оказались 737,7 тысячи строк с данными клиентов, в том числе 633 тысячи уникальных адресов

электронной почты, 315 тысяч телефонных номеров, а также хеши паролей. Во время написания этой статьи на одном из форумов появилась информация о крупной утечке базы данных страховой компании «Росгосстрах», якобы содержащей персональные данные клиентов, их медицинские анкеты и другую конфиденциальную информацию[3].

[3] На момент написания статьи еще не было официального подтверждения или опровержения информации об этой утечке.

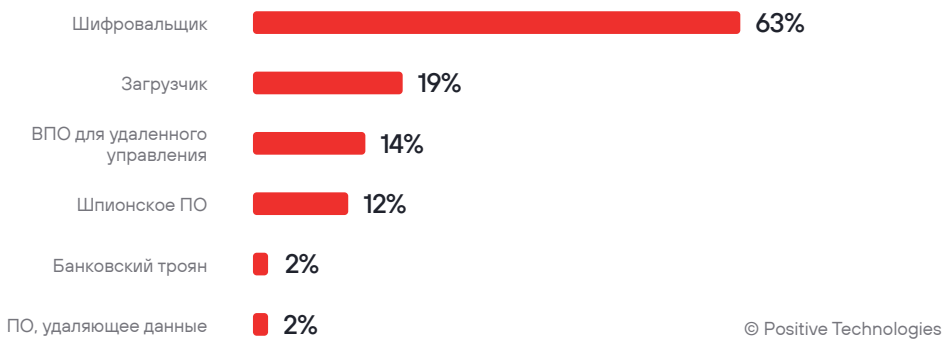
Рисунок 3. Сообщение об утечке 400 ГБ данных клиентов из компании «Росгосстрах»



Штрафы за утечку персональных данных в России недостаточно высоки, чтобы говорить о серьезном финансовом ущербе организаций в случае их наложения, но подобные инциденты негативно влияют на репутацию. К примеру, после сообщения о кибератаке и утечке конфиденциальных данных клиентов брокерской компании Angel One ее акции упали в цене на 2%.

Если говорить про российские банки, нельзя не отметить, что в 2023 году на фоне сложной геополитической обстановки они продолжают подвергаться мощным DDoS-атакам, которые направлены на временное нарушение работы цифровых сервисов. Регулятор отмечает лишь незначительное снижение их количества по сравнению с прошлым годом, когда наблюдался беспрецедентный всплеск активности преступников. В этом проявляется специфика российского банковского сектора на фоне общемировой тенденции, согласно которой основной причиной остановки работы финансовых сервисов становятся шифровальщики. Они существенно выделяются (63%) в статистике наиболее часто используемого в атаках вредоносного ПО. Для сравнения: годом ранее доля шифровальщиков составляла лишь 18%, а первую строчку занимали загрузчики с долей 59%.

Рисунок 4. Типы вредоносного ПО в успешных атаках на финансовые организации (Q1–Q3 2023)



Аналогичную тенденцию подтверждают и другие исследователи. Например, Sophos отмечает самый высокий за всю историю уровень атак программ-вымогателей в финансовой отрасли. По их наблюдениям, в 81% финансовых организаций в рамках киберинцидентов, связанных с атаками вымогателей, данные были успешно зашифрованы, и лишь 14% компаний удалось остановить атаку до того, как системы были заблокированы. По информации из того же исследования, в 25% успешных атак злоумышленники не только зашифровали данные, но и похитили их. Например, атака вымогателей LockBit на один из крупнейших банков Индонезии BSI привела к нарушению работы отделений банка и банкоматов. Злоумышленники потребовали выкуп в двадцать миллионов долларов, но получили отказ, после чего выложили в сеть полтора терабайта конфиденциальных данных банка.

Если рассматривать кибератаки в разрезе применяемых методов, можно отметить существенное снижение доли социальной инженерии (25%). В прошлогоднем исследовании ее доля составляла 47%. Это не означает снижения количества самих фишинговых атак, мы связываем это изменение с возросшей долей других методов: наблюдается значительное увеличение числа инцидентов, в которых использовались уязвимости ПО. В частности, значимый вклад в эту категорию внесли атаки с эксплуатацией уязвимости приложения для безопасной передачи данных MOVEit Transfer (CVE-2023-34362). Группировка CIOp активно эксплуатировала ее еще в начале года, а патч для закрытия бреши был выпущен только в мае. Большое количество инцидентов пришлось на второй и третий кварталы, когда эксплойт взяли в оборот и другие преступники. Это говорит о том, что далеко не все финансовые компании, использующие такое ПО (оно распространено в странах Северной Америки), вовремя среагировали на угрозу. Таким образом, в 2023 году компрометация финансовых организаций осуществляется не только классическими приемами (с помощью фишинговых сообщений), также активно используются уязвимости на сетевом периметре, приносящие хлеб так называемым брокерам первоначального доступа. Далее в исследовании мы покажем примеры объявлений о продаже таких доступов и оценим их стоимость на теневых площадках. Финансовым организациям необходимо выстроить надежную защиту внешнего сетевого периметра и повысить эффективность процесса управления уязвимостями.

Рассматривая наиболее распространенные методы атак, важно отметить и существенную долю инцидентов (22%), в которых ключевым способом компрометации стала атака на цепочку поставок.

Рисунок 5. Методы компрометации информационной инфраструктуры финансовых организаций (Q1–Q3 2023)

К примеру, эксперты Checkmarx выявили несколько успешных атак на цепочку поставок ПО с открытым исходным кодом в банковском секторе. В рамках одной из атак злоумышленники даже создали фейковую страницу на LinkedIn, где выдавали себя за сотрудника банка-жертвы, чтобы размещение вредоносных npm-пакетов не вызвало подозрений. Подобные атаки могут стать трендом ближайших лет, если учитывать тенденции на повсеместное использование ПО с открытым исходным кодом в собственных разработках компаний, в том числе в финансовых организациях.

Если резюмировать, можно выделить несколько важных тенденций:

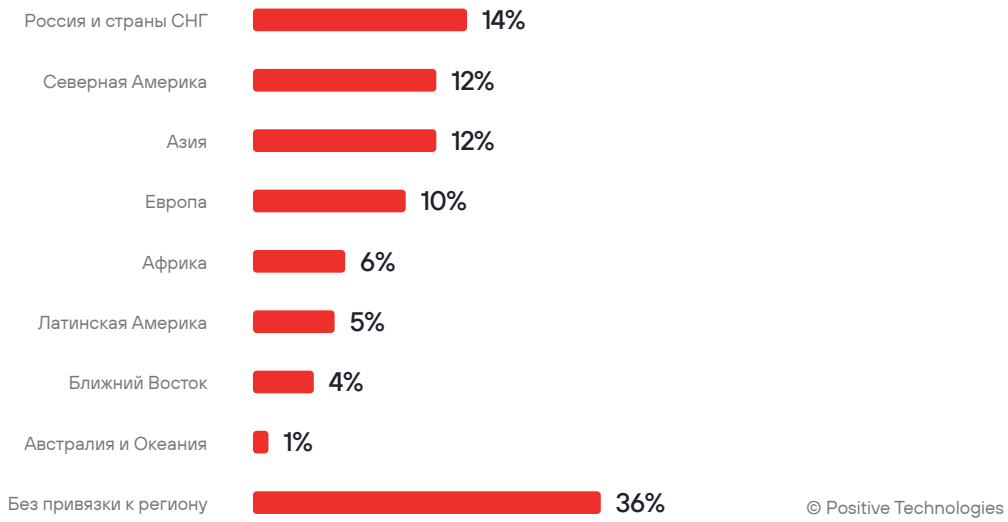
- Атаки упрощаются и при этом продолжают приносить немалую прибыль преступникам.
- Утечки баз данных несут существенные риски клиентам финансовых компаний, они способствуют повышению эффективности мошеннических схем преступников, потому что злоумышленник может в разговоре с жертвой назвать ее персональные данные, номера счетов и карт, а иногда и остатки по счету, что повышает доверие, а значит и вероятность успеха атаки.
- Атаки проводят не только финансово мотивированные преступники, но и хактивисты.
- Шифровальщики активно применяются для компрометации инфраструктуры финансовых организаций и наносят существенный ущерб бизнесу.
- Атаки с подменой npm-пакетов на вредоносные может стать серьезной угрозой для финансовых организаций, использующих в своих системах компоненты с открытым исходным кодом.

Оценка актуальных угроз будет неполной, если не проанализировать взгляд самих злоумышленников на финансовый сектор. Далее рассмотрим, какие темы наиболее ярко выделяются в общении преступников на теневых площадках.

Злоумышленники нацелены на данные клиентов

Анализ объявлений на тематических площадках в дарквебе и сообщений в профильных телеграм-каналах показал, что тренды, описанные выше, в большинстве своем находят отражение и в общении злоумышленников. Из их сообщений прослеживается не только специфика атак, но и география скомпрометированных компаний.

Рисунок 6. Распределение сообщений на теневых площадках по географии скомпрометированных организаций



Треть изученных объявлений (36%) содержат темы, не привязанные к какому-либо конкретному региону, в них преступникам неважно местонахождение жертвы. Но большинство сообщений о продаже или покупке товаров и услуг включают запрос или указание на вполне конкретный регион. Россия и страны СНГ находятся на первой строчке этого рейтинга ввиду особо острой геополитической обстановки, которая находит отражение и в киберпространстве. После начала специальной военной операции множество киберпреступных групп разделились на два лагеря, поддерживающих одну из сторон конфликта на Украине. В результате в сторону российских компаний, в том числе из финансового сектора экономики, оказались направлены масштабные атаки, обусловленные идеологическими мотивами (хактивизм). Злоумышленники пытались дестабилизировать состояние финансовой отрасли России не только путем вывода из строя банковских систем, но и с помощью подрыва доверия граждан к финансовой системе страны в целом. Попытки достичь таких целей заключались среди прочего в информационных вбросах (распространении фейковой информации) и в максимальном освещении каждого инцидента кибербезопасности, связанного с финансовыми учреждениями. Негативно настроенные в отношении России злоумышленники активно выкладывали в сеть утекшие базы данных, в итоге порядка 83% объявлений на теневых площадках, так или иначе связанных с российским финансовым сектором, посвящены

именно базам данных клиентов.

Рисунок 7. Распространение базы данных клиентов страховой компании «Ренессанс» на теневых площадках

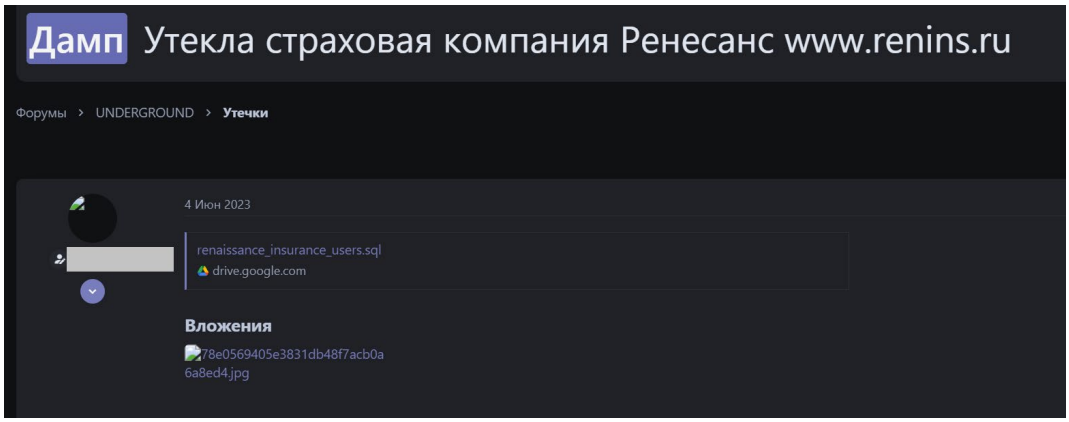


Рисунок 8. Распространение базы данных клиентов страховой компании «Согаз-Жизнь» в телеграм-канале

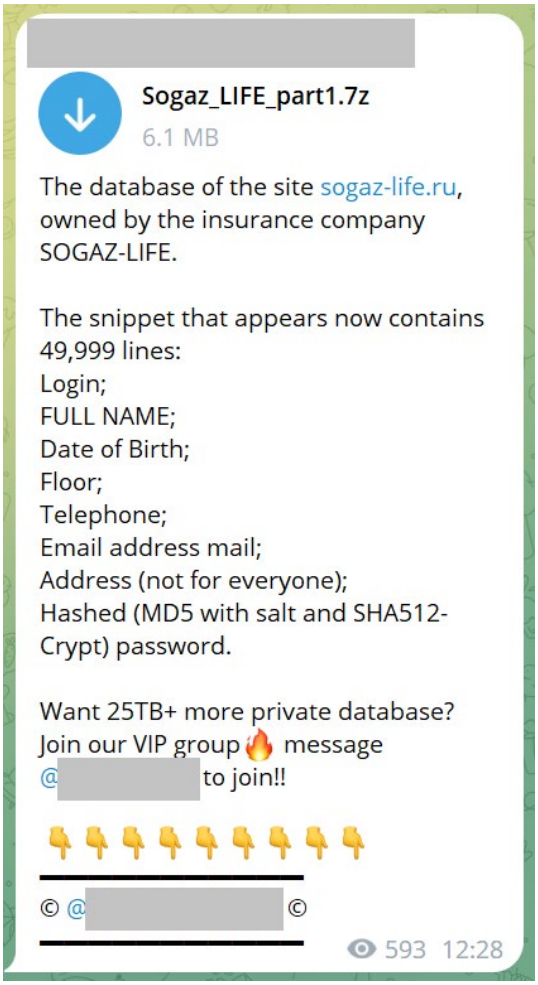
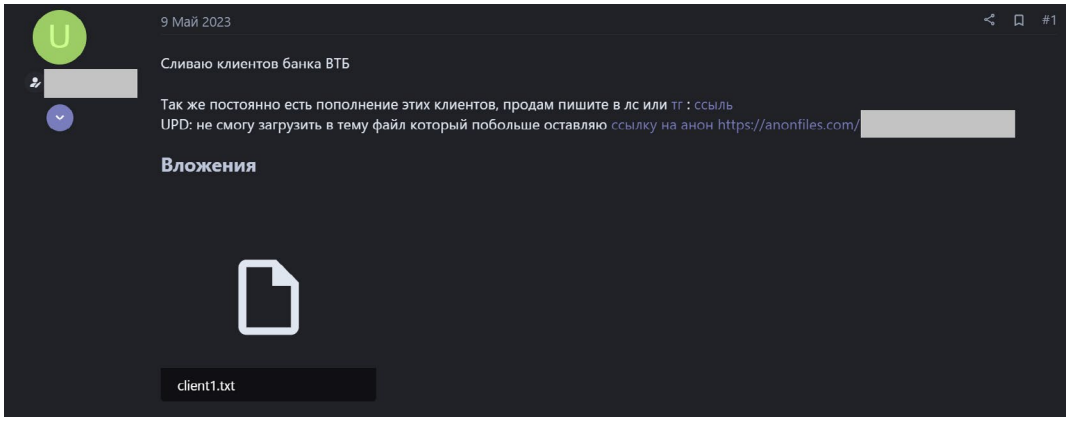
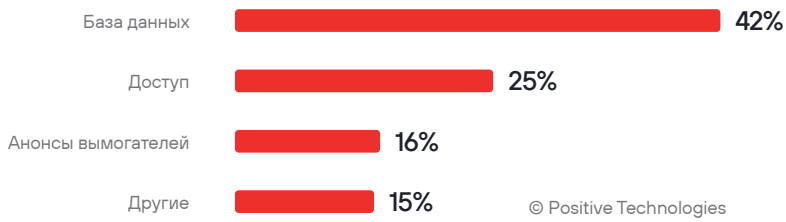


Рисунок 9. Объявление о продаже данных клиентов банка ВТБ



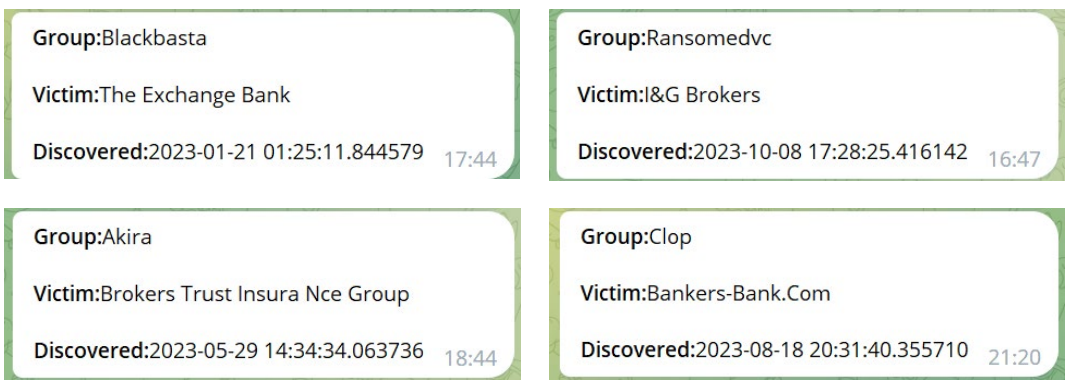
Общая статистика по всем изученным объявлениям также говорит о значительном внимании киберпреступников к данным клиентов финансовых компаний по всему миру. В 42% сообщений можно встретить объявление о продаже, покупке или бесплатной раздаче баз данных.

Рисунок 10. Тематика сообщений на теневых площадках в контексте атак на финансовые организации



Отдельно мы выделили категорию «Анонсы вымогателей» (ransomware), к которой относятся объявления о результатах активности преступных групп, промышляющих вымогательством в киберпространстве. В таких объявлениях авторы телеграм-каналов и веток на форумах агрегируют информацию о взломе очередной организации вымогателями, анонсируют скорую публикацию или выкладывают конфиденциальные данные жертв, не заплативших выкуп.

Рисунок 11. Примеры сообщений в телеграм-каналах о взломах финансовых учреждений вымогателями



В большинстве изученных сообщений (43%) базы данных распространяются бесплатно. Доли объявлений о покупке и продаже таких баз различаются незначительно. Продают, как правило, базы из свежих утечек крупных компаний либо услуги инсайдеров по предоставлению сведений о клиентах по запросу. В объявлениях о покупке в основном размещаются запросы на какие-то специфичные данные или конкретные компании, которые не были обнаружены среди активных предложений. Большая доля таких запросов (29%) объясняется нацеленностью злоумышленников на конкретные организации или группы организаций со схожей спецификой. По данным нашей статистики, именно целевые атаки преобладают в финансовом секторе (98% всех инцидентов).

Рисунок 12. Распределение сообщений о покупке и продаже баз данных клиентов финансовых организаций по типам

Цена в объявлении может быть указана как за всю базу целиком, так и в виде фиксированной стоимости за каждую строку. Одна строка базы обойдется покупателю примерно в пять долларов. Стоимость половины баз из проанализированных источников не превышает одной тысячи долларов, но в зависимости от объемов и значимости для злоумышленников содержащейся в базе информации цена может доходить до десяти тысяч и даже значительно превышать эту сумму.

Рисунок 13. Стоимость баз данных на теневых площадках ($)

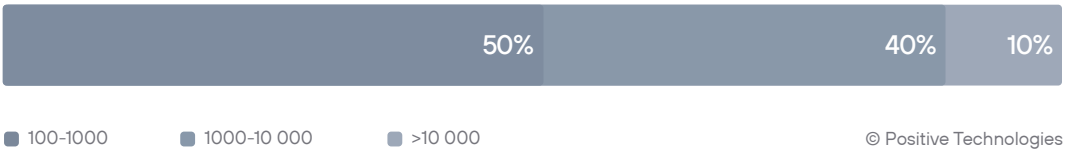


Рисунок 14. Объявление о покупке базы клиентов банка с построчной оплатой

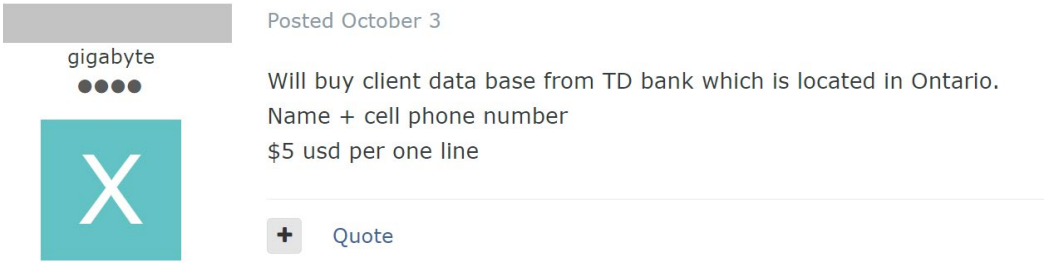
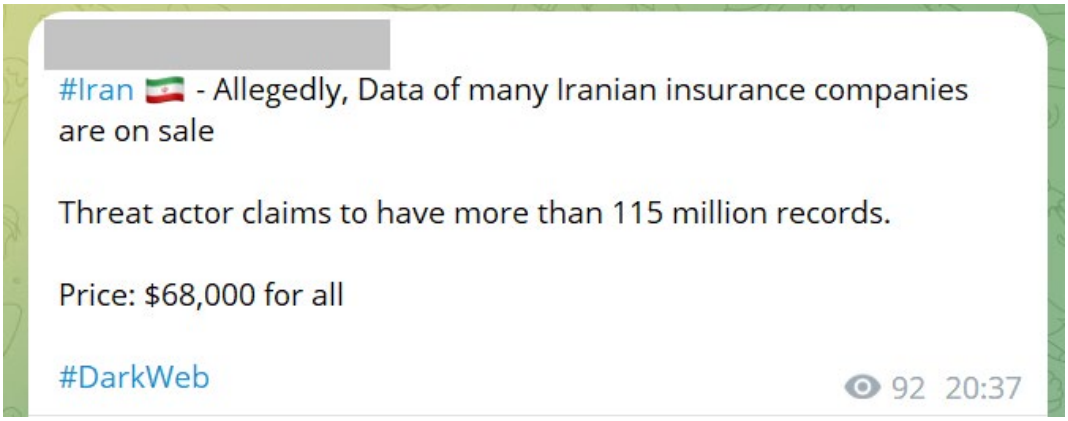


Рисунок 15. Объявление о продаже баз данных иранских страховых компаний



Купленные базы используются в дальнейших атаках на клиентов финансовых организаций методами социальной инженерии, а также для подбора учетных записей, если в такой базе содержались учетные данные (например, идентификаторы и хеши паролей). С каждой новой утечкой у преступников появляется дополнительная информация о потенциальных жертвах, они могут агрегировать разные базы, обогащая уже собранную информацию. В результате преступники вполне могут собрать такую коллекцию информации, которая позволит им получить подробный цифровой образ жертвы[4] и использовать эти данные в мошеннических схемах или для дальнейшей перепродажи.

Доступы по-прежнему в цене

Не менее ценным товаром на рынке преступных услуг являются первоначальные доступы[5] в информационную инфраструктуру финансовых организаций. Речь о торговле доступами заходит в каждом пятом изученном объявлении. Еще в 2020 году мы обратили внимание на тренд, который назвали «доступ на продажу» (в различных источниках можно встретить также термин «доступ как услуга»), позднее мы исследовали динамику развития этого тренда.

Сегодня доступы активно продаются на теневых рынках наравне с персональными данными и вредоносным ПО, причем предложение (90% объявлений) значительно превышает долю объявлений о покупке (10%). Это может говорить о том, что количество уже реализованных проникновений в сети финансовых компаний столь велико, что преступникам нет необходимости размещать объявления о покупке: они могут получить нужные им доступы из уже существующих предложений на рынке. Сообщения о покупке обычно содержат заказы на конкретные организации или специфичные банковские системы.

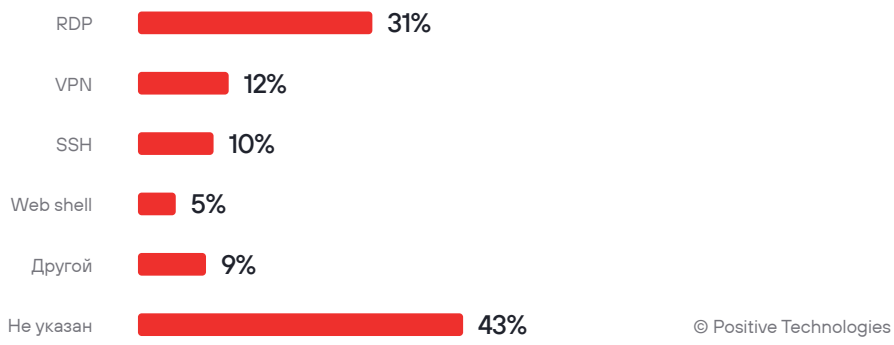
[4] Под цифровым образом в этом случае понимается набор данных, позволяющий полностью идентифицировать личность в цифровом пространстве (идентификаторы и сканы документов, удостоверяющих личность, номер водительского удостоверения, контактные данные, дата и место рождения, медицинская информация, номера страхования, номера банковских счетов и кредитных карт, остатки по счету, информация о кредитах, имуществе и другие данные).

[5] Доступ как объект продажи на теневом рынке — это собирательное понятие, включающее в себя ПО, эксплойты, учетные данные и все остальное, что позволяет несанкционированно управлять конкретным удаленным устройством или множеством устройств.

Рисунок 16. Объявление о покупке доступа к серверу приложений платежного коммутатора (payment switch)

На форумах в дарквебе представлены доступы разных типов. Наиболее распространены доступы по протоколам RDP, VPN и SSH, так как позволяют выполнять команды операционной системы на атакованном узле интерактивно, обычно скомпрометированный компьютер или сервер расположен во внутренней инфраструктуре организации. Менее распространены доступы посредством веб-интерпретатора командной строки (web shell), который обеспечивает выполнение команд через скомпрометированное веб-приложение и представляет собой веб-оболочку. Доступ через web shell также дает злоумышленнику контроль над сервером, но обычно такой сервер размещен на внешнем сетевом периметре, а не в локальной сети, и команды выполняются в неинтерактивном режиме, что ограничивает набор возможных действий. Преступникам потребуется развивать атаку для получения более удобного, скрытного и стабильного канала управления.

Рисунок 17. Типы доступов, которыми торгуют на теневых площадках



Перечисленные типы подключений, как правило, предоставляют злоумышленнику локальные привилегии (административные или пользовательские) на конечном устройстве. Это наиболее распространенный (38% и 16% соответственно) уровень привилегий в объявлениях о продаже. Ценность такого доступа напрямую зависит от значимости того сервера или компьютера, к которому возможно подключиться. Наиболее широкие привилегии нарушитель получит, если завладеет доступом уровня администратора домена Active Directory (12% объявлений). Такие привилегии

позволят ему развивать атаки на все критически важные системы, подключенные к домену, в том числе компьютеры ключевых сотрудников компании и бизнес-системы. Столь высокий уровень доступа получить намного сложнее, чем локальный на отдельных серверах, так как потребуется не только проникнуть во внутреннюю сеть организации, но и закрепиться в ней, остаться незамеченным и развить атаку, поэтому стоимость такого доступа выше, а предложения о продаже встречаются реже.

Рисунок 18. Уровень привилегий из объявлений о торговле доступами на теневых площадках

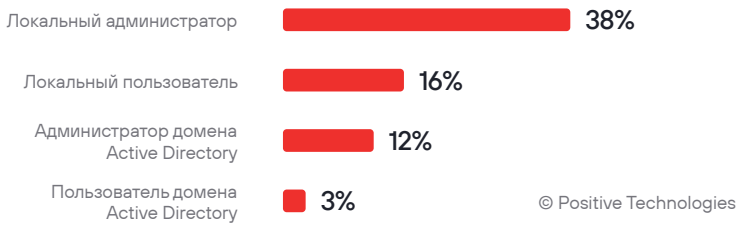


Рисунок 19. Объявление о продаже доступа с привилегиями администратора домена

Рисунок 20. Объявление о продаже доступа с привилегиями системы на узле с Windows

Стоимость большинства доступов не превышает одной тысячи долларов, что обусловлено широким распространением доступов с локальными привилегиями. Но дорогостоящие предложения вовсе не редки. Например, в одном из объявлений предлагается к покупке привилегированный доступ к домену крупного банка за 15 биткоинов (на момент размещения объявления эта сумма была эквивалентна нескольким сотням тысяч долларов).

Рисунок 21. Стоимость первоначальных доступов на теневых площадках ($)

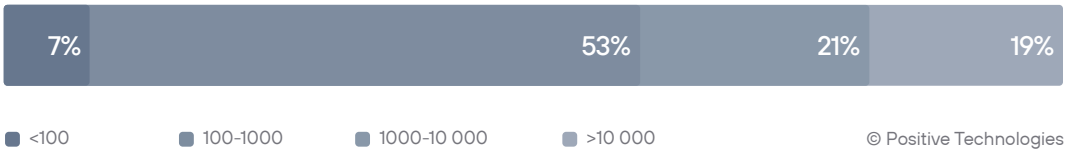
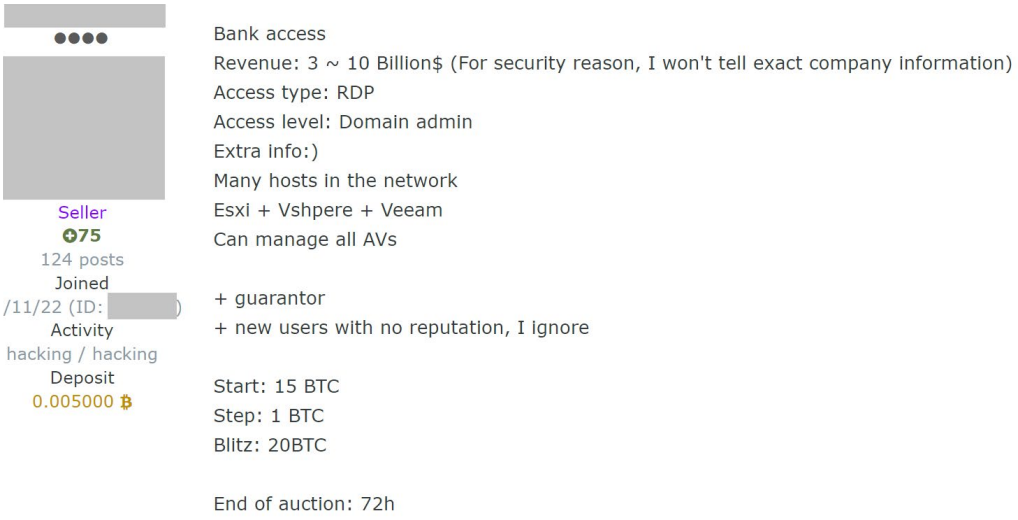


Рисунок 22. Предложение о продаже привилегированного доступа в сеть крупного банка



Дорогостоящие предложения о продаже доступа в сети некредитных финансовых организаций встречаются реже. Предположительно, это обусловлено тем, что, в отличие от некредитных финансовых организаций, из банков потенциально можно украсть не только множество конфиденциальной информации и данные клиентов для последующих атак на них, но и непосредственно крупные суммы с корреспондентского счета.

Рисунок 23. Стоимость доступов в сети банков ($)

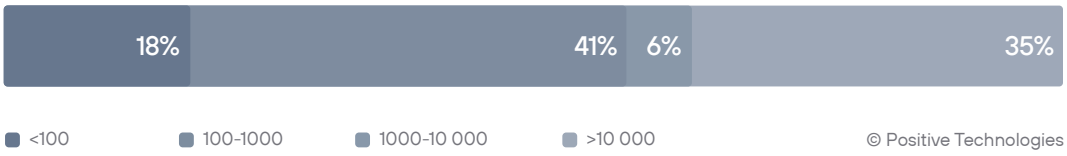
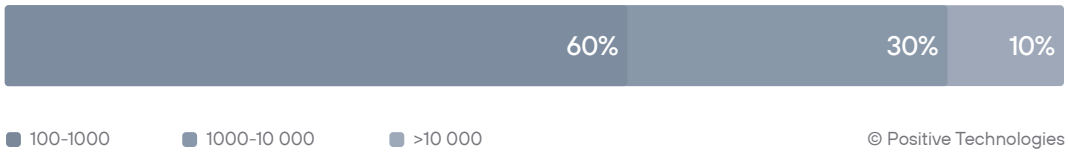


Рисунок 24. Стоимость доступов в сети некредитных финансовых организаций ($)



Рассмотренные выше примеры и цифры демонстрируют серьезную проблему защищенности сетевых периметров компаний по всему миру. Мы проверили и подтвердили это на практике. Результаты тестирований на проникновение в сети финансовых организаций, проведенных нашими экспертами в 2023 году, свидетельствуют о том, что внешний злоумышленник может получить доступ к корпоративной локальной вычислительной сети всех протестированных банков. Во всех случаях были проэксплуатированы уязвимости ПО, доступного для подключения из интернета, а самая старая из них была известна еще с 2017 года. Лишь в одном из банков периметр был защищен так качественно, что для проникновения потребовалось выявить и проэксплуатировать уязвимость нулевого дня (0-day). Это подтверждает тезис о том, что внешний замотивированный злоумышленник всегда найдет способ проникновения даже в хорошо защищенный банк. В связи с этим крайне важно обеспечить такую систему безопасности, которая позволит исключить возможность нанесения неприемлемого ущерба бизнесу финансовой организации даже в случае проникновения нарушителя.

Выводы

Кража денег из банка с помощью кибератаки — сложная задача для преступников: им требуются глубокие знания систем и процессов финансовой организации. Другое дело — кража информации, поэтому злоумышленники активно сливают конфиденциальные данные из сетей компаний, монетизируют утечки, атакуя клиентов финансовых организаций с помощью полученных сведений. Чем больше баз оказывается в руках преступников, тем более подробные коллекции данных они могут составить. Они повышают эффективность социотехнических атак за счет формирования подробного цифрового образа жертвы. Финансовым организациям необходимо уделить особое внимание этой проблеме.

В эту сторону должны внимательно смотреть и регуляторы. Например, в Европе уже много лет действует общий регламент защиты персональных данных — General Data Protection Regulation (GDPR), несоблюдение которого влечет большие штрафы в случае утечки данных. В России наказание за утечку существенно мягче и не рассматривается организациями как серьезный риск для бизнеса. К примеру, штраф за крупную утечку данных клиентов сети медицинских лабораторий «Гемотест» в 2022 году составил всего шестьдесят тысяч рублей. Однако важно отметить и положительные тенденции. Комиссия кабинета министров Российской Федерации по законопроектной деятельности поддержала проект поправок к Кодексу РФ об административных правонарушениях, повышающий штраф за утечку персональных данных и устанавливающий оборотные штрафы в случае повторной утечки вплоть до 500 миллионов рублей. Регулятор финансовой отрасли также не остался в стороне: Центральный банк России с 1 октября 2023 года обязал банки предлагать своим клиентам страхование от мошеннических списаний средств со счетов. Необходимо продолжать развивать этот вектор, но учитывать и возможные негативные

последствия таких изменений. С одной стороны, высокие штрафы за утечки могут сыграть на руку преступникам, требующим выкуп за неразглашение: они могут повысить ценник. С другой стороны, при возникновении риска уплаты крупного штрафа у компании, допустившей утечку, может быть больше мотивации заплатить деньги преступникам, а не надзорным органам.

Если говорить об угрозах для самих финансовых организаций, то злоумышленники продолжают уже устоявшуюся традицию вымогательства за восстановление систем и неразглашение утечек, а также активно монетизируют результаты своих атак, продавая готовые доступы другим преступникам. Кроме того, финансовым компаниям необходимо обратить пристальное внимание на угрозу, связанную с распространением вредоносных пакетов под видом легитимных компонентов ПО с открытым исходным кодом. Разработчикам необходимо отслеживать зависимости в своем коде и проверять заимствованный код на наличие закладок и уязвимостей.

Не теряет свою актуальность хактивизм, особенно в отношении российских компаний на фоне специальной военной операции на Украине и обостренной геополитической ситуации в мире. Важно отметить, что основная цель преступников — дестабилизация финансовой системы страны в целом, несмотря на то что они атакуют отдельные компании. Злоумышленники стремятся посеять панику среди населения, вызвать недоверие граждан к финансовым институтам и государственной власти. Это — угроза отраслевого уровня, поэтому решить такую проблему отдельным предприятиям не под силу. Необходим централизованный подход с участием отраслевого центра компетенции, роль которого в России сегодня выполняет ФинЦЕРТ. Координация реагирования на отраслевом уровне, основанная на понимании неприемлемых последствий в масштабах всей отрасли, а также анализ возможных цепочек событий, которые могут к таким последствиям привести, помогут выработать и реализовать эффективный план по нейтрализации подобных угроз.

ptsecurity.com
pr@ptsecurity.com