

экономика региона

От киберпреступника до шпиона

Количество киберпреступлений в Сибири в 2019 году выросло на четверть в сравнении с предыдущим годом, достигнув 16 тыс. уголовных дел. Большую долю от всех кибератак по-прежнему занимают кражи конфиденциальной информации для перепродажи. Однако в последнее время, отмечают эксперты рынка, растет число правонарушений с целью шпионажа. Это обусловлено ростом ценности информации и развитием цифровизации. Киберпреступность становится глобальной и более опасной, чем традиционная организованная преступность. При этом группы хакеров становятся все быстрее и технологичнее, не ограничены в перемещениях и могут атаковать жертву, находясь в любой точке земного шара.

— технологии —

В прошлом году правоохранители Сибирского федерального округа завели на 4 тыс. больше уголовных дел, совершенных с использованием информационных технологий или в сфере компьютерной информации, чем в 2018-м, когда их было более 12 тыс. Таким образом, доля киберпреступлений в общем количестве зарегистрированных преступлений, предусмотренных ст. 159 УК РФ (мошенничество), в округе достигла 63%, сообщили в МВД России.

Кража и продажа конфиденциальной информации на черном рынке, включая персональные данные пользователей и клиентов организаций и госструктур, сегодня являются основной целью киберпреступников, подтверждает руководитель направления аналитики и спецпроектов специализирующейся на информационной безопасности компании InfoWatch Андрей Арсентьев.

«В 2019 году во всем мире киберпреступники стали активнее использовать фишинговые атаки (вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям), причем не только по электронной почте, но и через другие каналы», — говорит господин Арсентьев.

В России ежедневно проводится до 1250 успешных фишинговых атак, связанных с открытием неизвестных вложений. В 2018 году таким образом хакерами было похищено более 200 млн руб., сообщили в сервисе «Автоматика» госкорпорации «Ростех».

Согласно отчету экспертов специализирующейся на расследовании киберпреступлений компании Group-IB, атаки чаще всего совершаются на банки, страховые компании, телеком, ТЭК и госпредприятия.

Индустриальные предприятия и системы промышленной автоматизации в ближайшем будущем все чаще будут становиться жертвами кибератак. «Предпосылки: растущий интерес киберпреступников к индустриальным организациям и недооценка степени риска самими предприятиями», — считают эксперты компании «Лаборатория Касперского», специализирующейся на разработке систем защиты от компьютерных вирусов.

В то же время, говорит директор по развитию бизнеса по информационной безопасности МРФ «Сибирь» ПАО «Ростелеком» Денис Поршин, будет наблюдаться всплеск вредоносной активности и в отношении ритейла. «Киберпреступники могут преследовать самые разные цели: прямой вывод денежных средств, повреждение, кража и компрометация критичных данных, кибершпионаж, останова или прерывание бизнес-процессов компании-жертвы, включение ее серверов в бот-сеть для совершения дальнейших атак и т. п. Поиск путей монетизации говорит о том, что в состав группировок входят не только технические исполнители, но и аналитики», — считает господин Поршин.

Прежде чем начать атаку, злоумышленники проводят оценку ROI (коэффициент окупаемости), чтобы понять, насколько целесообразна та или иная атака. «Например, казалось бы, финансовая индустрия — целевая для киберпреступников, но банки вкладывают значительные средства в безопасность, и для успешной атаки потребуются много времени и ресурсов. Поэтому иногда вместо того, чтобы тратить деньги и время на атаку, которая скорее всего не будет успешной, киберпреступники ориентируются на отрасли, которые традиционно мало инвестируют в безопасность и обновление оборудования и программного обеспечения. Это здравоохранение, образование



Действия сотрудников (умышленные и случайные) в Сибири в 2019 году привели к 80% случаев утечек информации

и гостиничный бизнес. Их легче взломать, они могут с большей вероятностью заплатить выкуп за продолжение работы, и у них точно есть конфиденциальная информация о клиентах, пациентах», — полагает эксперт по информационной безопасности компании Avast Луис Корронс.

Денис Поршин при этом отмечает, что инструментарий киберпреступников совершенствуется. Злоумышленники проникают в инфраструктуру при помощи как социальной инженерии (метод несанкционированного доступа к информации или системам хранения информации без использования технических средств), так и вредоносного ПО (программного обеспечения).

Кроме этого, хакеры сегодня стали чаще, атаковав инфраструктуру, незаметно находиться в ней, чтобы детально исследовать и получить как можно более глубокий доступ к информационным и технологическим системам.

Долгое время до 98% всех киберпреступлений, по оценкам Group-IB, были связаны с кражей денег. Однако в последние годы эксперты отмечают стремительное увеличение преступлений, совершенных с целью шпионажа, саботажа и диверсии. Например, для причинения ущерба репутации компании, частичной или полной остановки ее деятельности.

«Самая главная угроза, с которой мир столкнется в ближайшее время, — кибертерроризм. Если большую часть своей истории компьютерная преступность в основном была финансово мотивирована, то есть старалась разными способами зарабатывать деньги, то приблизительно с 2014 года все чаще о себе стали заявлять группы, чей целью является кибершпионаж и кибертерроризм», — комментируют эксперты Group-IB.

Зайти через сотрудника

Главные виновники утечек — это по-прежнему рядовые сотрудники. В России их действия (умышленные и случайные) в 2019 году привели к 72% случаев распространения информации от общего количества, в Сибирском федеральном округе — почти к 80%. В глобальном масштабе около 50% утечек за 2019 год произошло по вине хакеров, сообщили в ГК InfoWatch.

Исследуя утечки на основе публичных сообщений, аналитики нашей группы компаний пришли к выводу, что в 2018 году виновниками 9,5% из них в России и 8,8% в Сибири были хакеры. По предварительным данным нашего экспертно-аналитического центра, в 2019 году доля хакеров среди виновников утечек по всей России составила 18,5%, а в Сибири — 12,5%, — сообщил Андрей Арсентьев.

Согласно данным Group-IB, русскоговорящая преступность длительное время создавала почти 80% сложных технологических схем в мире, а все новое ВПО (вредоносное программное обеспечение), шаблоны и сценарии целенаправленных атак тестировались именно на российских банках. Сейчас пять групп представляют реальную угрозу финансовому сектору: Cobalt, Silence, MoneyTaker — Россия, Lazarus — Северная Корея, SilentCards — новая группа из Кении.

В причастности к одной из этих групп правоохранители подозревают 25-летнего задержанного администратора бот-сетей из Новокузнецка, который заразил несколько тысяч компьютеров российских и зарубежных пользователей с помощью трояна Pony Formgrabber, предназначенного для кражи учетных записей. Расследование в 2019 году провели сотрудники МВД при участии экспертов Group-IB. Задержанный оказался «наемником» и предлагал киберкриминальным группам услуги по модели cybercrime-as-a-service: на арендованных серверах разворачивал, тестировал и обслуживал административные панели троянов, а также сам похищал учетные записи (логины и пароли, сохраненные в почтовых клиентах и браузерах) для продажи на подпольных форумах.

Используя троян Pony Formgrabber, преступная группа Toplel атаковала клиентов российских банков в 2014–2015 годах и в 2017 году.

За настройку одной административной панели для управления вредоносными программами, по словам задержанного, он получал в среднем 1–5 тыс. руб., деньги ему переводили в криптовалюте. Хакер специализировался на троянах класса RAT (remote access toolkit), которые позволяли получить полный доступ к зараженному компьютеру. «На жаргоне киберпреступников заразить машину трояном RAT называлось «бросить крысу»», — пояснили эксперты Group-IB.

«Когда я настраивал такие серверы, я понимал, что они могут использоваться для несанкционированного доступа к компьютерам других людей для копирования персональных данных», — признался задержанный. Кому хакер продавал эту информацию, он не знает: «Люди, которые откликались на мои объявления на хакерских форумах, имели только псевдонимы». Эксперты Group-IB не исключают, что украденные данные, которые задержанный продавал на форумах, киберпреступники могли использовать для рассылки спама, заражения вредоносными программами, различного рода мошеннических действий или кражи денег.

Задержанному предъявлено обвинение по ч. 1 ст. 273 УК РФ (создание, использование и распространение вредоносных компьютерных программ), он полностью признал вину. Ведется следствие.

Незрелая подготовка

Зрелость компаний в области кибербезопасности растет, но, к сожалению, недостаточно быстро. Это касается и компаний России в целом, и Сибири в частности. «Основные причины этого состоят в том, что бизнес часто не умеет просчитывать риски от кибератак и потому не отдает себе отчет в необходимости киберзащиты. Из этого следует, что и бюджеты на информационную безопасность выделяются в недостаточном объеме», — говорит Денис Поршин.

В то же время стопроцентной защиты от кибератак не существует, уверены эксперты рынка IT. И добавляют, что это возможно только в случае полного отказа от обработки информации с использованием компьютеров. «Не бывает абсолютно защищенной системы. Где-то есть технические уязвимости, где-то бреши в киберобороне связаны с недостаточной компетенцией сотрудников, а где-то действуют вредители», — отмечает директор по инфобезопасности IT-холдинга TalentTech Иван Дмитриев.

Главное заблуждение состоит в уверенности, что о кибербезопасности можно подумать когда-нибудь потом, отмечают эксперты. «Угрозы реальны, и защищаться от них важно уже на первоначальном этапе работы организации», — подчеркивает руководитель группы по кибербезопасности компании Softline в Сибири Иван Озеров.

Сегодня мир идет в сторону интернета вещей (IoT), и если умный чайник вряд ли доставит много проблем, то перехват управления цифровой электрической подстанцией, системой водоснабжения города или потоком транспорта может принести ощутимый ущерб. «Проблемой является и человеческий фактор, а точнее низкая осведомленность о базовых правилах информационной безопасности, таких как использование сложных паролей хотя бы на некоторых критичных системах, игнорирование вложений от неизвестных отправителей», — уверен эксперт концерна «Автоматика» госкорпорации «Ростех».

Так, МРСК Сибири (энергохолдинг «Росети Сибирь») с 28 февраля на 1 марта 2019 года подверглась мощным DDoS-атакам на оборудование перед XXIX Всемирной зимней Универсиадой в Красноярске. Количество одновременно атакующих узлов держалось на уровне 18 тыс. в течение суток. Атаки были остановлены при помощи специального сервиса для защиты от DDoS и атак на web-приложения. Кто стоял за этими действиями, в компании не говорят, отметив лишь, что адресное пространство на 90% ресурсов, с которых происходили атаки, принадлежит Китаю. «Однако это вовсе не значит, что данные IP-адреса не эксплуатировались из любой другой страны», — отметили в энергохолдинге.

После этого инцидента компания усилила киберзащиту, доработав комплексную систему информационной безопасности. Стоимость одной такой атаки эксперты оценили в \$3–5 в зависимости от продолжительности и интенсивности.

По данным исследования компании «Лаборатория Касперского», средний ущерб от успешной кибератаки в России для компаний среднего и малого бизнеса составляет 4,3 млн руб., для крупного бизнеса — 14,3 млн руб.

Количество кибератак растет, а вот раскрываемость таких преступлений пока не демонстрирует позитивную динамику. Как подсчитали в прокуратуре Томской области, доля раскрываемости мошенничеств, совершенных при помощи информационных технологий, не превышает 12%. «Так, в 2017 году в регионе их раскрыто 12%, в 2018 году — 11,4%, в 2019 году — 10,8%», — сообщил заместитель прокурора Томской области, старший советник юстиции Александр Ткаченко.

Чтобы защититься от киберпреступников, бизнесу и государственным структурам нужно применять системный подход, отмечают игроки рынка IT. Выстраивать эшелонированную и адаптивную систему защиты информации, постоянно развивать и совершенствовать ее. «Очень важно также развивать сотрудников: понимание кибербезопасности — один из ключевых навыков в 2020 году для каждого, кто работает с компьютером, и многие работодатели обучают этому свою команду. Главное — не отставать от киберпреступности более чем на шаг», — говорит директор по инфобезопасности IT-холдинга TalentTech Иван Дмитриев.

Киберпреступники совершенствуются, становятся быстрее и технологичнее, они не ограничены в перемещениях, могут атаковать из любой точки земного шара. Количество их атак растет, в том числе на небольшие предприятия. Вместе с тем увеличивается и количество жалоб пользователей госуслуг и клиентов различных структур и бизнеса на утечку в сеть конфиденциальных данных. Так, по данным Роскомнадзора, в 2019 году от жителей Сибирского федерального округа поступило более 4,5 тыс. обращений, в том числе 4 тыс. по вопросу защиты их данных. В аналогичном периоде 2018-го — 3,5 тыс. Прирост составил 983 обращения (28%).

При этом из всего объема рассмотренных обращений информация о нарушениях подтвердилась лишь в 5% случаев (за аналогичный период 2018 года — в 7%), сообщили в ведомстве. Ответственные за хранение конфиденциальной информации понимают важность работы по ее защите, уделяя все больше внимания этому вопросу.

Лолита Белова