«МАРКЕТИНГ» СЕТЕВЫХ ШАНТАЖИСТОВ

Насколько нынешняя жизнь не представляется без компьютера и цифровых технологий, настолько же опасной в современном мире оказывается киберпреступность. Если всего несколько лет назад сетевым грабежом промышляли в основном хакеры-студенты, которые вредили в интернете из чистого хулиганства, то теперь электронные разбойники объединяются в масштабные преступные группировки.

Преступники придумывают новые способы вскрывать информационные системы: печальный «хит» последних месяцев – так называемые программы-вымогатели, которые в одночасье превращают ценную информацию в компьютере в мусор, если не заплатить (впрочем, если вымогателям платить, то все равно чаще всего данные пропадают).

Самое тревожное, что, помимо экономических преступлений в банковской и общественной деятельности, электронные атаки начали широко использоваться против обычных людей. В связи с этим эксперты «Лаборатории Касперского» поделились своим видением развития сложных угроз и целевых атак, так называемых Advanced Persistent Threats (APT) в 2020 году.

Прогнозы были сделаны на основе инцидентов, которые специалисты наблюдали на протяжении последних месяцев. Выявленные тенденции предполагают, что угрозы станут более скрытыми и целенаправленными, а распространение новейших технологий, таких как, например, машинное обучение и нейросети, выведет сложность кибератак на новый уровень.

По оценкам экспертов, в самое ближайшее время возникнет опасность утечек особенно ценной информации – например, биометрических данных человека. Персональная информация пользователей

помогает злоумышленникам совершенствовать свои методы социальной инженерии, так что их интерес к чужим личным данным будет только возрастать. Помимо этого, киберпреступники вполне могут начать применять искусственный интеллект для профилирования жертвы и создания информационных подделок, так называемых deepfake, которые уже сегодня достаточно широко обсуждаются.

В последнее время злоумышленники стали отходить от практики массового распространения универсальных программ-вымогателей и более тщательно выбирают своих жертв – другими словами, они ищут те компании, которые будут готовы заплатить значительные суммы за восстановление своих данных. По предположениям экспертов, в ближайший год это **«целевое вымогательство» будет набирать обороты и, возможно, станет более агрессивным.** Например, вместо шифрования файлов злоумышленники могут начать угрожать жертвам публикацией украденных данных. Кроме того, в попытках диверсифицировать свои атаки с помощью программ-вымогателей киберпреступники могут избрать мишенями не самые очевидные устройства – умные телевизоры, часы, машины, дома и т. п.

Одной из особенностей APT-атак является их скрытость. Злоумышленники старательно маскируют свои «следы» и нередко расставляют так называемые «ложные флаги», чтобы пустить исследователей по неверному следу. И, как полагают в «Лаборатории Касперского», эта тенденция продолжит свое развитие. **Киберкриминальные группы будут стремиться не только избежать атрибуции, но и выставить виноватым кого-либо еще.** Для этого они могут, например, намеренно использовать бэкдоры, которые ассоциируются с другими APT-группировками, или специально сливать свой код, чтобы им воспользовались другие атакующие и еще больше запутали общую картину.

По мнению антивирусного эксперта Дмитрия Галова, ни один прогноз, даже самый тщательный, не может предусмотреть всего, что, возможно, случится в будущем. Среды, в которых разворачиваются атаки, настолько обширны, а обстоятельства так многогранны, что будущее развитие угроз наверняка будет сложнее самых хороших прогнозов.

– Тем не менее это не отменяет того, что мы продолжим следить за развитием APT-угроз и стоящих за ними злоумышленников и будем стараться еще лучше понимать их методы, предугадывать их действия и возможные последствия, – отметил Дмитрий Галов.

Все чаще жертвами программ-шифровальщиков становятся медицинские компании. В связи с этим специалисты «Лаборатории Касперского» составили ряд прогнозов на 2020 год относительно киберинцидентов, связанных с медицинскими учреждениями. По их мнению, в даркнете будет появляться все больше объявлений о продаже медицинских данных, в том числе информации из медицинских карт или страховых полисов. Уже сейчас они иногда стоят дороже, чем данные банковских карт, поскольку являются ценным ресурсом для злоумышленников, которые используют их, чтобы входить в доверие к пользователям, обманывать их самих или их родственников.

Доступ к данным электронных медицинских карт может быть интересен не только для кражи. Злоумышленники потенциально могут вносить в них изменения, чтобы совершать целевые атаки и намеренно затруднять постановку диагнозов. Такие инциденты становятся возможными, потому что, во-первых, в индустрии здравоохранения недостаточно серьезно воспринимают риски, сопряженные с цифровизацией, а во-вторых, не уделяют должное внимание вопросам обучения сотрудников базовым навыкам кибербезопасности.

Скажем, в 2019 году в медицинских организациях по всему миру было атаковано каждое пятое устройство (19 %). По прогнозам «Лаборатории Касперского», число подобных атак будет расти, особенно в развивающихся странах, где только начинается процесс цифровизации таких услуг. Это чревато нарушениями в постановке диагноза и даже лишением пациентов помощи, которая требуется немедленно.

Кроме того, увеличится число атак на научно-исследовательские медицинские институты и фармацевтические компании, проводящие инновационные исследования. Так,

в 2019 году были атакованы 49 % устройств в фармацевтических компаниях. Исследования, проводимые такими организациями, стоят дорого, и результаты их ценятся высоко, поэтому, скорее всего, в 2020 году они все чаще будут становиться мишенью APT-группировок, специализирующихся на краже интеллектуальной собственности.

– Мы регулярно исследуем различные медицинские устройства и видим, что их безопасность находится на удручающе низком уровне. В будущем это чревато серьезными рисками. Готовиться к отражению целевых атак медицинским учреждениям нужно уже сейчас, и начинать стоит с тренингов по кибербезопасности для врачей и медсестер, которые работают с этими устройствами, – отмечает антивирусный эксперт Дмитрий Галов.

Эксперты «Лаборатории Касперского» обнаружили еще одну схему киберзлоумышленников, которые обернули в свою пользу политику начисления штрафов для компаний за утечки данных. Мошенники обещают пострадавшим пользователям денежную компенсацию, но, чтобы получить ее, необходимо купить временную социальную страховку. Этот вид скама* эксплуатируется не только в России, но и в Беларуси, Алжире, Египте, ОАЭ и других странах. Преступники действуют от имени выдуманной организации – Фонда защиты персональных данных, якобы основанного Федеральной торговой комиссией США. На специально созданном фейковом сайте сообщается, что этот фонд выплачивает компенсации пользователям, пострадавшим от утечек данных, и получить их могут граждане любой страны. Пользователю предлагается проверить, не оказались ли его личные данные

в общем доступе: для этого нужно указать имя, фамилию, телефонный номер и свои страницы в социальных сетях. После этого сообщается, что его данные, в том числе фотографии, видео, контакты, были обнаружены в одной из утечек, что дает право на компенсацию, исчисляемую в тысячах долларов США. Затем мошенники просят ввести номер социального страхования SSN, но, независимо от того, вводит ли пользователь настоящий номер или сообщает об его отсутствии, сайт выдает уведомление об ошибке и предложение купить временный за 9 долларов США. Жертва перенаправляется в форму оплаты – русско- или англоязычную, в зависимости от IP-адреса пользователя. Цена указывается соответственно либо в рублях, либо в долларах.

– Авторы этой схемы, вероятно, говорят на русском языке, так как отдельные ее составляющие очень похожи на те, что в последнее время используются в скаме в России и странах СНГ, – комментирует Татьяна Сидорина, старший контент-аналитик «Лаборатории Касперского». – Производятся рассылки и объявления о возможности выиграть крупную сумму в лотерею, получить вознаграждение за опрос, выплаты от пенсионного фонда, хорошо оплачиваемую работу диспетчером такси. В них предлагают легкие деньги, но для их получения всегда нужно внести небольшую сумму, необходимую якобы в качестве комиссии или закрепительного платежа. Теперь к этим рассылкам добавилась и схема, эксплуатирующая проблемы, связанные с утечками личных данных, – объясняет она.

Чтобы не попасться на удочку скамеров, «Лаборатория Касперского» рекомендует пользователям:

• скептически относиться к предложениям получить те или иные выплаты: если кто-то обещает большую сумму за нечто простое, вроде участия в опросе, стоит насторожиться, а уж если от вас требуют какие-либо предварительные выплаты, это с высокой долей вероятности мошенничество;

• всегда проверять, существует ли на самом деле организация, которая предлагает выплаты, и, если существует, внимательно вычитывать ее сайт, обращать внимание на то, не пестрит ли он грамматическими и орфографическими ошибками – реальная компания не допустит большого количества ошибок и опечаток на своих ресурсах;

• использовать надежное защитное решение, такое как Kaspersky Internet Security, для всесторонней защиты от широкого спектра угроз.

** Скам – мошеннические рассылки и объявления, в которых пользователям обещают крупное денежное поступление за выполнение любых несложных действий, например за участие в акции или прохождение опроса и т. д. Однако для получения обещанных выплат человеку необходимо сначала перевести организаторам небольшую сумму денег, якобы за оплату комиссии или под другим предлогом.*