Атаки вируса-шифровальщика Sodinokibi на компании Европы и США привели к росту числа обращений за выплатами страховок от киберрисков, сообщает Financial Times (FT). Как поясняет FT, целью вируса являются англоязычные страны, которые рассматриваются создателями шифровальщика как наиболее платежеспособные.

Sodinokobi не атакует компании из стран бывшего СССР, цитирует FT специалиста по кибербезопасности страховой компании Тома Беннетта. Россию этот шифровальщик практически не затронул, констатирует руководитель отдела исследования и детектирования сложных угроз «Лаборатории Касперского» Антон Иванов. Шифровальщик проверяет используемую раскладку клавиатуры и если установлен определенный язык, то он не шифрует файлы жертвы, объясняет эксперт. Русский язык входит в этот список.

Отраслевых предпочтений у Sodinokobi нет. Малый и средний бизнес он атаковал через компании, обслуживавшие их IT-инфраструктуру, сообщает FT.

Уроки выучены

Вирусы-шифровальщики блокируют доступ к компьютерной системе организации и требуют от нее выкуп (как правило, в криптовалюте биткойн) в обмен на доступ к данным. Наиболее громкие атаки шифровальщиков произошли в 2017 г.: это были вирусы WannaCry и NotPetya. По данным Positive Technologies, шифровальщики составляют 13% всех типов вредоносного программного обеспечения. Однако новый шифровальщик, пиковая активность которого пришлась на июнь и июль, требует более крупные выкупы, чем обычно: средний размер выкупа Sodinokibi составил $150 000 по сравнению с $50 000 для других типов вирусов, пишет FT.

Массовые эпидемии 2017 г. заставили крупный бизнес существенно инвестировать в безопасность и сейчас они защищены от 90% существующих типов программ-шифровальщиков, которые массово распространяются злоумышленниками, уверен директор блока экспертных сервисов компании Bi.Zone («внучка» Сбербанка, занимающаяся кибербезопасностью) Евгений Волошин. В России большинство заражений шифровальщиками приходится на малый и средний бизнес, который уделяет меньше внимания кибербезопасности. Некоторые из них годами присутствуют в инфраструктуре предприятий, рассказывает Волошин.

В мире WannaCry остается самым распространенным шифровальщиком, детектируемым решениями «Лаборатории Касперского», говорит Иванов. По данным компании, общее число уникальных пользователей, атакованных шифровальщиками во II квартале 2019 г., выросло по сравнению с январем – июнем 2018 г. на 46% и превысило 230 000. Бывает, что в важных компонентах инфраструктуры не установлен защитный софт или обновления операционной системы, объясняет он.

Полис против хакера

По данным страховщика AIG, за 2018 г. в регионе EMEA (Европа, Ближний Восток и Африка – Россия входит в этот регион) вирусы-вымогатели стали причиной 18% заявлений по убыткам комплексного страхования киберрисков, говорит старший

андеррайтер по финансовым рискам AIG в России Петр Дорофеев. Сумма выкупа по российскому законодательству не страхуется: в сумму покрытия входят расходы на проведение расследования и минимизацию последствий атаки, уточняет он. В России количество договоров комплексного страхования от киберрисков растет, констатирует начальник департамента страхования финансовых институтов компании «Греко ДжейЭлТи. Страховые брокеры» Дмитрий Грузинцев. Если в 2018 г. было заключено около 10 таких договоров, то в 2019 г. – уже 20, утверждает эксперт. По наблюдениям Грузинцева, страховками киберрисков интересуются крупные промышленные предприятия и небольшие IT-компании.

Ущерб от киберпреступности неуклонно растет, а вклад вирусов-вымогателей остается стабильно высоким, рассказывает руководитель управления финансовых рисков «Альфастрахования» Анастасия Селезнева. По ее словам, ни одна отрасль не может чувствовать себя защищенной, поскольку атаки вымогателей часто бывают неизбирательными.

Рынок страхования киберрисков перспективен. По оценкам «Сбербанк страхования», он может вырасти с нынешних нескольких десятков миллионов рублей в год до 8–10 млрд руб. к 2025 г. Основной спрос на услугу будут формировать малые и средние предприятия, а также физические лица – пользователи смартфонов. Бизнес опасается утечки данных и простоев производства из-за DDoS-атак. Средний ущерб от киберинцидента для крупных компаний составляет 11 млн руб., для малого и среднего бизнеса – 1,6 млн руб., оценивало «Сбербанк страхование».

Ведомости, 13 августа 2019 г.