Дважды на одни грабли или поучительная история о ransomware

Одна организация, пав жертвой вируса-шифровальщика, заплатила вымогателям несколько миллионов, чтобы быстрее восстановить заблокированные файлы. Однако в компании не извлекли урока из случившегося, что вскоре привело к повторной ransomware-атаке. О поучительной истории рассказали в Национальном центре кибербезопасности Великобритании (NCSC). Кому именно дважды посчастливилось наступить на одни и те же "киберграбли", не уточняется.

По данным NCSC, сумма выкупа в биткоинах, который заплатила организация, по текущему курсу составила бы без малого 6,5 миллиона британских фунтов или около 8,8 миллиона долларов США. Получив от вымогателей дешифровщик для восстановления файлов, компания не стала ничего предпринимать, чтобы разобраться в произошедшем и обезопасить свою сеть. В итоге менее чем через две недели те же самые хакеры снова атаковали свою жертву, используя для внедрения вируса-шифровальщика тот же механизм, что и прежде. В компании не нашли другого выхода, кроме как снова заплатить вымогателям.

Специалисты британского центра безопасности подчеркивают, что для жертв ransomware приоритетной задачей, наряду с восстановлением данных, должно быть установление причин, которые позволили киберпреступникам проникнуть в сеть незамеченными и внедрить вредоносное ПО.

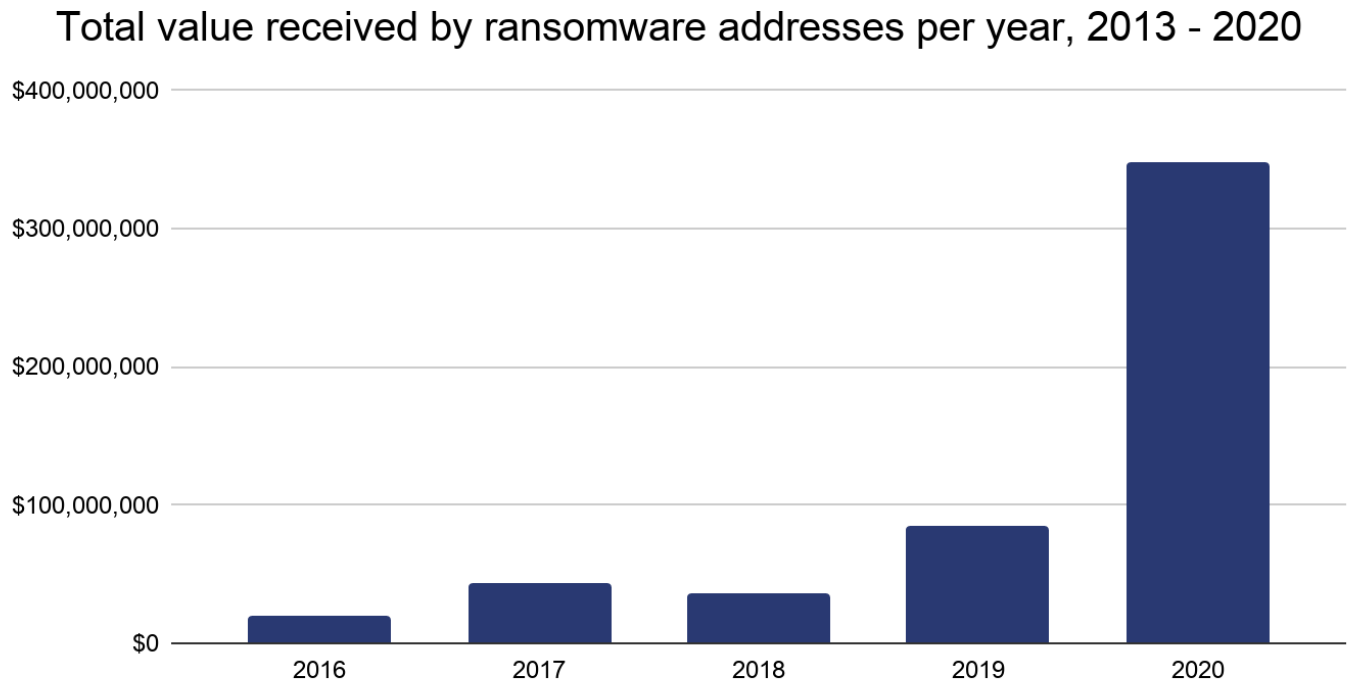
˝Вирус-шифровальщик часто бывает видимым симптомом гораздо более серьезного вторжения в сеть, произошедшего за несколько дней до атаки или даже раньше. Лечить следует причину болезни, а не ее признаки˝, - говорят в NCSC.

Даже если удалось обезвредить вирус-шифровальщик и восстановить компьютерные системы с помощью резервных копий, хакеры могут оставить лазейки для проникновения в сеть. Например, обладая правами администратора, злоумышленникам не составит труда повторно внедрить шифровальщик.

Устранение последствий ransomware-атаки - зачастую длительный и дорогостоящий процесс. Расследование инцидента, восстановление систем и данных могут занять до нескольких недель, а убытки для бизнеса нередко измеряются миллионами, даже если жертва не платит выкуп. Учитывая это, ИБ-эксперты призывают компании заранее думать о киберзащите своих сетей, своевременно обновлять операционные системы и устанавливать патчи безопасности, а также применять многофакторную аутентификацию.

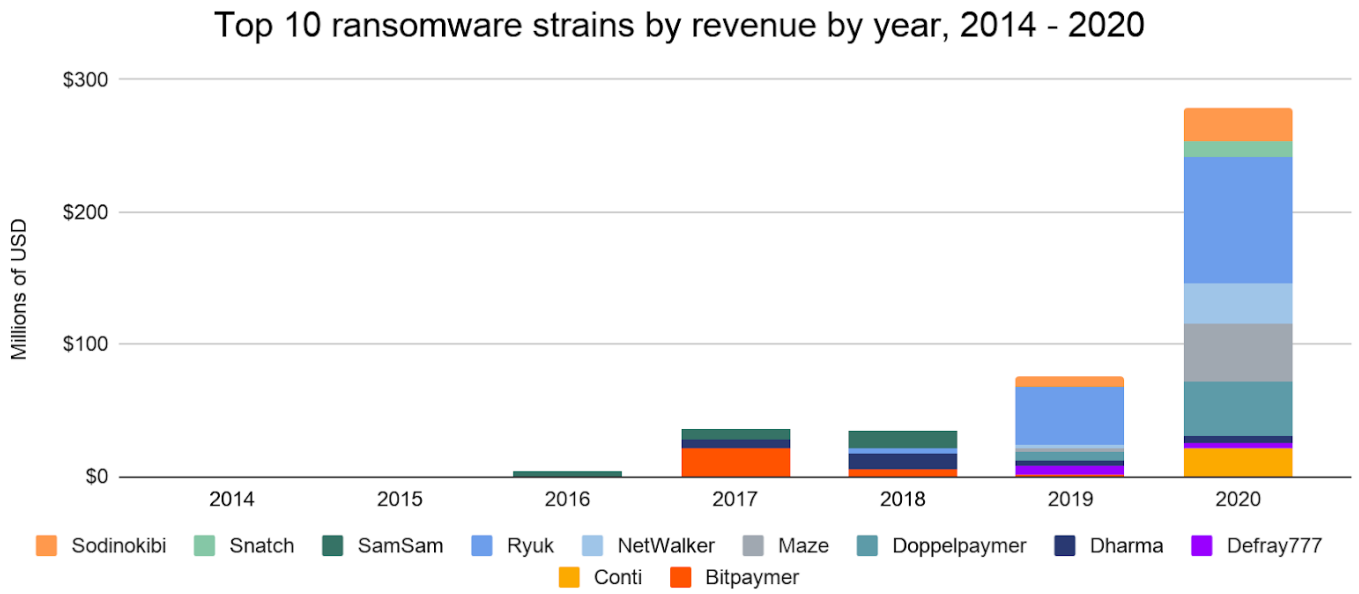
Кроме того, организациям рекомендуется регулярно создавать резервные копии систем и хранить их оффлайн, чтобы в случае успешной атаки вируса-шифровальщика можно было восстановить сеть с минимальными потерями.

Хотя советы достаточно тривиальные, в мире по-прежнему немало компаний, которые ими пренебрегают. Хватает и тех, кто, вопреки рекомендациям специалистов по кибербезопасности, выполняет требования о выкупе при заражения вирусом-шифровальщиком. Об этом, в частности, говорят данные из недавнего отчета компании Chainalysis, которая специализируется на отслеживании криптовалютных транзакций.

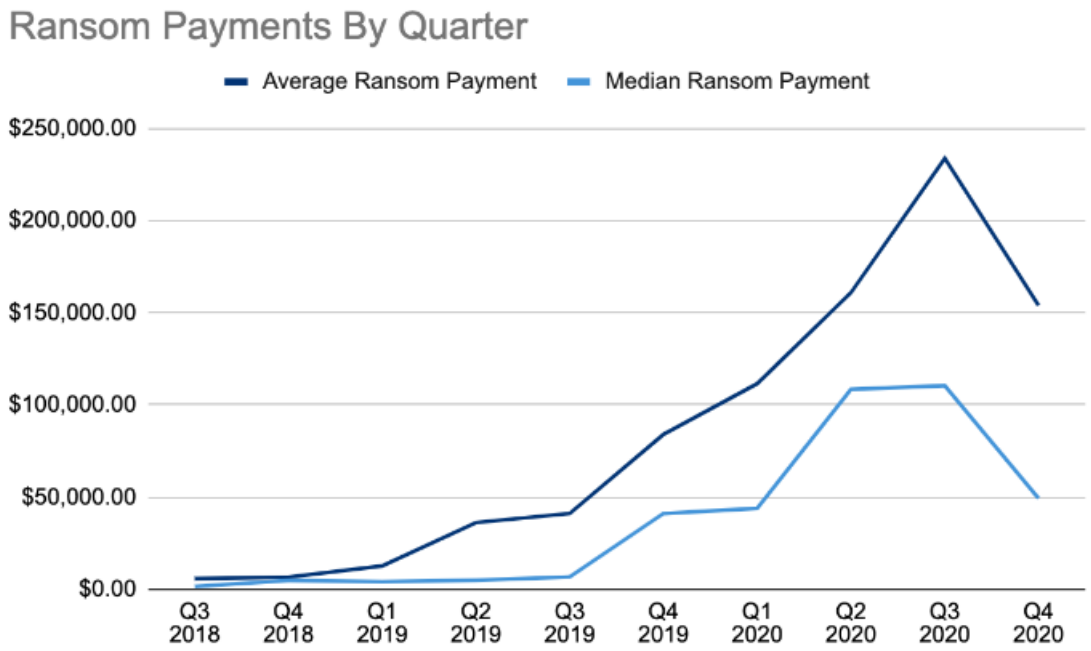


Проанализировав активность блокчейн-адресов, которые засветились во время ransomware-атак, специалисты подсчитали, что общая сумма выплат кибервымогателям в 2020 году выросла на 311% и достигла 350 миллионов долларов. В Chainalysis отмечают, что реальная цифра, скорее всего, выше, поскольку далеко не все компании публично признаются в том, что стали жертвами успешной атаки вымогательского ПО.

Наиболее прибыльными вариантами ransomware, согласно анализу Chainalysis, в минувшем году были Ryuk, Maze, Doppelpaymer, Netwalker, Conti и REvil (он же Sodinokibi). Шифровальщики Snatch, RansomExx / Defray777 и Dharma показали меньшую отдачу, но все равно принесли своим хозяевам миллионы.



В то время как в Chainalysis говорят о стремительном росте платежей кибервымогателям, из другого недавнего исследования выяснилось, что средняя сумма выкупа за последнее время существенно уменьшилась. ИБ-компания Coveware, помогающая решать проблемы из-за ransomware-атак, в свежем отчете за IV квартал 2020 года сообщила, что пострадавшие от вымогательского ПО все чаще отказываются платить преступникам. По этой причине средний размер выкупа в октябре-декабре уменьшился на треть и составил чуть больше 154 тысяч долларов против почти 234 тысяч долларов тремя месяцами ранее.

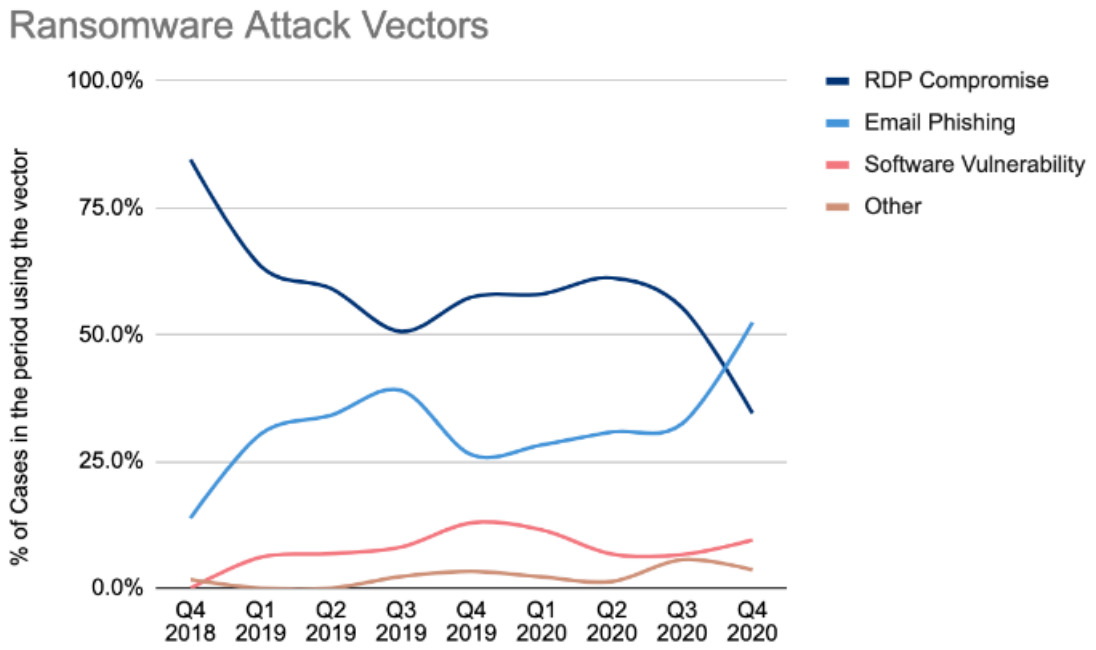


Видя растущее нежелание платить выкуп, кибервымогатели чаще прибегают к тактике, при которой наряду с шифрованием данных происходит их кража. Чтобы сделать жертву сговорчивее и заставить выполнить требования, преступники угрожают выложить конфиденциальную информацию в Сеть. Статистика Coveware показывает, что в IV квартале 70% всех ransomware-атак осуществлялось по такой схеме, тогда как в предыдущей четверти их доля составляла 50%. Впрочем, и этот метод теряет действенность: если в третьем квартале требованиям кибервымогателей уступили почти 75% компаний, которым угрожали разглашением данных, то в октябре-декабре уже менее 60% жертв согласились заплатить выкуп.

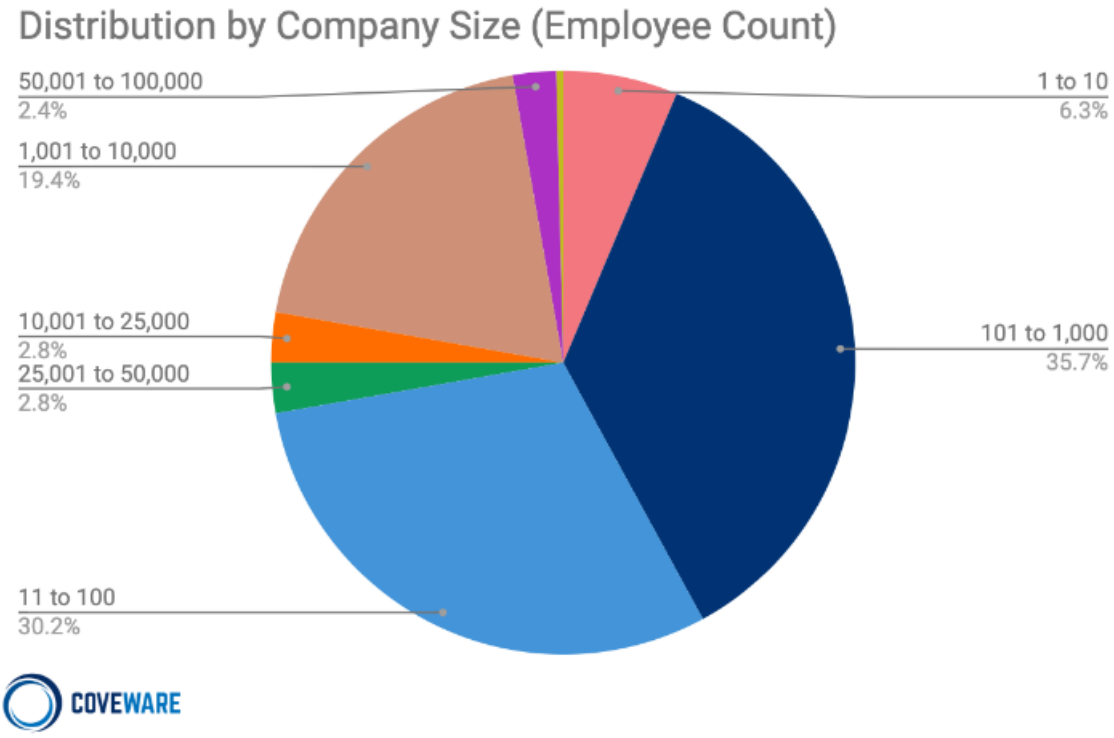
Как и прежде, специалисты Coveware не рекомендуют поддаваться угрозам вымогателей, поскольку это поощряет преступников продолжать атаки. Также следует помнить, что уплата выкупа совершенно не гарантирует, что похищенные данные будут удалены. Есть риск, что преступники не выполнят обещания стереть файлы, либо другие злоумышленники, имевшие доступ к похищенной информации, могут вновь попытаться воспользоваться ею для шантажа.

В исследовании Coveware перечислены 16 наиболее часто встречающихся вариантов вымогательского ПО, которые используются в рамках все более популярной у киберпреступников бизнес-модели ″ransomware-атака как услуга″ (Ransomware as a Service, RaaS). Среди них Sodinokibi, Egregor, Ryuk, Netwalker, Maze, Conti v2, DopplePaymer, Conti. Suncrypt, Zeppelin, Avaddon, Phobos, Nephilim, MedusaLocker, Lockbit и GlobeImposter 2.0.

Самыми распространенными методами внедрения вымогательского ПО по-прежнему остаются фишинговые рассылки по электронной почте и заражение через внешние службы удаленного доступа, прежде всего через Remote Desktop Protocol (RDP).



Данные Coveware показывают, что целью ransomware-атак чаще становятся небольшие или средние компании, у которых реже есть специальный персонал, занятый обеспечением ИТ-безопасности. Судя по статистике, жертвами ransomware-атак постоянно становятся компании из сферы профессиональных услуг, особенно небольшие юридические и финансовые фирмы.



В IV квартале 2020 года в штате организаций, атакованных вымогательским ПО, в среднем насчитывалось 234 сотрудника, что на 39% больше по сравнению с показателем предыдущей четверти. Такая популярность компаний среднего размера у вымогателей объясняется тем, что в ИТ-сети таких жертв, как правило, проще проникнуть, а их платежеспособность выше, чем у совсем небольших фирм.